NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

STATE METHODS FOR A CYBER INCIDENT

by

Michael R. Mulligan

March 2012

Thesis Advisor:	Richard Bergin
Thesis Co-Advisor:	Ted Lewis

Approved for public release; distribution is unlimited

Reissued 2 Jul 2013; distribution downgraded from "U.S. Government Agencies Only" to public release.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE State Methods for a Cyber Incident	5. FUNDING NUMBERS
6. AUTHOR(S) Michael R. Mulligan	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The National Cyber Incident Response Plan stipulates the state homeland security advisor as the contact point for a significant cyber incident. But this may not be the most effective method of response because the state homeland security advisors are not domain experts for cyberspace. A questionnaire was sent to state chief information officers and/or state chief information security officers to determine current capability and procedures for responding to a national cybersecurity incident. Nineteen states replied with 227 responses relating to information sharing between states and the federal government; use of established cybersecurity event and response definitions, coordination and control mechanisms, and terms; use of risk-based approaches to cyber incident planning, including remediation based on workflows and procedures; establishment of thresholds when predefined boundaries are crossed; and instigation of varying courses of action. As a result of the survey, the author recommends increasing knowledge and information flow between state and federal agencies regarding national cyber incidents; the establishment of regional cybersecurity hubs throughout the nation; and the creation of a national cyber incident teleconferencing network and prearranged protocols for situational awareness and communication of courses of action following a cybersecurity incident.

14. SUBJECT TERMS National Cyber Incident Response Plan, State Information Security Officer, Cyberspace, Cybersecurity, Department of Homeland Security Office of Cybersecurity and Communications, National Cybersecurity and Communications Integration Center	15. NUMBER OF PAGES 147
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

STATE METHODS FOR A CYBER INCIDENT

Michael R. Mulligan
Director Operations and Planning, DHS Office of Cybersecurity and Communications
B.S., California Polytechnic University, 1989
M.S., National Graduate School, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2012

Author: Michael R. Mulligan

Approved by: Richard Bergin
Thesis Advisor

Ted Lewis
Thesis Co-Advisor

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The National Cyber Incident Response Plan stipulates the state homeland security advisor as the contact point for a significant cyber incident. But this may not be the most effective method of response because the state homeland security advisors are not domain experts for cyberspace. A questionnaire was sent to state chief information officers and/or state chief information security officers to determine current capability and procedures for responding to a national cybersecurity incident. Nineteen states replied with 227 responses relating to information sharing between states and the federal government; use of established cybersecurity event and response definitions, coordination and control mechanisms, and terms; use of risk-based approaches to cyber incident planning, including remediation based on workflows and procedures; establishment of thresholds when predefined boundaries are crossed; and instigation of varying courses of action. As a result of the survey, the author recommends increasing knowledge and information flow between state and federal agencies regarding national cyber incidents; the establishment of regional cybersecurity hubs throughout the nation; and the creation of a national cyber incident teleconferencing network and prearranged protocols for situational awareness and communication of courses of action following a cybersecurity incident.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACSA	Applied Computer Security Associates
AEIT	Agency for Enterprise Information Technology
AVIEN	Anti-Virus Information Exchange Network
BITS	Bureau of Information Technology Services
CDP	Cyber Disruption Plan
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNCI	Comprehensive National Cybersecurity Initiative
CRKI	Critical Resource Key Infrastructure
CSADA	Critical Supervisory and Data Acquisition
CS&C	Cybersecurity and Communications
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSSP	Control Systems Security Program
DEMA	Department of Emergency Management and Military Agency
DHS	Department of Homeland Security
DMS	Department of Management Services
DOD	Department of Defense
DOIT	Department of Information Technology
EAS	Emergency Alert System
EISA	Energy Independence and Security Act
EO	Executive Order
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
GFIRST	Government Forum of Incident Response and Security Teams

HSAS	Homeland Security Advisory System
HSEEP	Homeland Security Exercise and Evaluation Program
HSEM	Homeland Security and Emergency Management
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IACSS	International Association for Computer Systems Security, Inc.
ICS	Incident Command System
ICS-CERT	Industrial Control Systems–Cyber Emergency Response Team
IPAWS	Integrated Public Alert and Warning System
ISIRT	Information System Incident Response Team
ISO	Information Security Officer
ISOC	Information Security Operations Center
ITB	Information Technology Bulletin
ITSG	Information Technology Security Group
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCC	National Coordinating Center
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NCPEC	National Coalition for the Prevention of Economic Crime
NCRAL	National Cyber Risk Alert Level
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Council
NESCO	National Electric Sector Cybersecurity Organization
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NJIC	National Joint Information Center
NOAA	National Oceanic and Atmospheric Administration
NOC	National Operation Center

NPS	Naval Post Graduate School
NRF	National Response Framework
NSPD	National Security Presidential Directive
NTAS	National Terrorism Advisory System
NWS	National Weather Service
OA	Office of Administration
OIS	Office for Information Security
OIT	Office Information Technology
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PO	Privacy Officer
POC	Point of Contact
RCPGP	Regional Catastrophic Preparedness Grant Program
SANS	System Administration, Audit, Network, Security Institute
SEOC	Security Operation Center
SERRP	Statewide Emergency Response and Response Plan
SIPC	State Infrastructure Protection Center
SIRT	Security Incident Response Team
SIRT	State Incident Response Team
SISPO	Statewide Information Security and Privacy Office
SOP	Standard Operating Procedure
SWAT	Special Weapons and Tactics Teams
US-CERT	United States Computer Emergency Readiness Team
WHO	World Health Organization

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Gregory Schaffer, Assistant Secretary Office of Cybersecurity and Communications, Department of Homeland Security, and his Chief of Staff, Paul Mesterhazy, for allowing me the time away to participate in the Naval Postgraduate Masters Program.

Key to this research was the support and input received from the state chief information officers and state chief information security officers.

Also important was the guidance and input received from my advisors, Richard Bergin, NPS faculty, and Ted Lewis, Executive Director, NPS Center for Homeland Defense and Security.

I would also like to acknowledge my colleagues in Cohort 1003/1004, who provided their insights and friendship during our distant learning segments and while in residence in the West Virginia hills during class and in the evening around a table at a local establishment.

Finally, and most importantly, thanks to my incredibly talented artist wife, Michelle, for her support and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. SUMMARY

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyberthreats require the engagement of the entire society. This includes government, law enforcement, the private sector, and most importantly, members of the public.

To address the states' role, this research reviewed the states' cybersecurity engagements for cyber incident responses to national significant cyber incidents. "National Significant Cyber Incidents" will be defined later.

Through a series of questions posed to the states and a literature review, the research was designed to understand response constructs, risk models, and alerting methodologies that could support states for a national significant cyber incident. The responses to the questions posed to the states produced beneficial cyber incident response patterns that could be implemented into planning efforts. The use of the beneficial cyber incident response patterns could also produce common procedures and terms. The recommendations in this research provide a means to better prepare the entire cyberspace society against the emerging threats by increasing knowledge and information flow regarding cyber incidents.

Chapter I looks at this dynamic cyberspace environment, its interconnectedness, its multifaceted responsibilities, and the scope and scale of the challenge to secure it.

B. BACKGROUND

1. Cyberspace

Cyberspace is defined as "a global domain consisting of the interdependent network of information technology infrastructures [that] includes the Internet, telecommunications networks, computer systems, and embedded processors and

controllers in critical industries" (United States Department of Homeland Security, Office of Cybersecurity and Communications [DHS-CS&C], 2011). "The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society" (White House Office of the Press Secretary, 2009). Cyberspace is vital to the functioning of our nation and national security. Furthermore, cyberspace encompasses our nation's economy, commerce, public safety, personal social networks, and many more activities. Government agencies, industry, and the public have become dependent on it.

Cyberspace is a dynamic and constantly changing ecosystem-like environment that cannot be treated as static. This environment includes many government agencies that provide direction and procedures to secure the nation from adversarial threats and vulnerabilities. The Energy Independence and Security Act of 2007 (EISA) states that the Commerce Department's National Institute of Standards and Technology is directed to "coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems" (Help Net Security, 2010). The Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery afterwards, and to ensure that first responders have access to effective communication services. (Federal Communications Commission [FCC], 2010). The cybersecurity mission of the Federal Bureau of Investigation (FBI) is to stop those behind the most serious computer intrusions and the spread of malicious code. On the FBI's public site this mission area is attributed to the National Strategy to Secure Cyberspace, signed by the president in 2003 (Federal Bureau of Investigation [FBI], 2010). The Department of Defense (DOD) has the U.S. Cyber Command, a subordinate unit of another DOD organization called U.S. Strategic Command. This command will direct the operations and defense of specified Department of Defense information networks and prepare to, when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace, and deny the same to our adversaries (McMichael, 2010). Finally, Homeland Security Presidential

Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," states the following: "The [Department of Homeland Security] Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace**.** The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations" (United States Department of Homeland Security [DHS], 2003).

2. Cyberspace Threats

The cyberspace environment is under perpetual attack. Cybersecurity threats against the United States are increasing. Reports of security incidents are on the rise, increasing over 650 percent over the past five years for federal agencies (United States Government Accountability Office [GAO], 2011, p. 8). Our interconnected threats to the cyberspace environment affect the public, private, and government sectors. Cyberspace allows us to communicate with our mobile devices; obtain a seat for air travel; power our homes, offices, and factories; maintain our personal banking and national economy; and obtain government services. Its benefits are tremendous and undisputed. The cyberspace user community is facing a set of emerging cybersecurity threats that are the result of increasingly sophisticated and persistent methods of attack.

President Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) in January 2008 (National Security Council, 2008). The CNCI consisted of a number of initiatives to establish a secure cyberspace for the United States. Moreover, in February 2009, President Obama initiated an interagency cybersecurity review to develop a strategic framework to ensure that the CNCI was being appropriately coordinated with Congress and the private sector. In May of 2009, President Obama issued the Cyberspace Policy Review or the "cyberspace 60-day review," as it is sometimes called. (White House, 2009).

Cybersecurity has been called “one of the most urgent national security problems facing the new administration” (Center for Strategic and International Studies, 2008). The Obama administration has declared that U.S. critical information infrastructures are a strategic national asset.

3. Cyberspace Incident Planning

The DHS Office of Cybersecurity and Communications (CS&C) works cooperatively to secure and ensure the availability of our nation’s cyber and telecommunications infrastructure. The Secretary of the DHS, through CS&C, is responsible for providing crisis management and coordination in response to significant cyber incidents; coordinating and integrating information from the federal cybersecurity centers, state, local, tribal, and territorial governments, and the private sector; and generally maintaining an organization to serve as a focal point for the security of cyberspace. DHS’s operational cybersecurity mission includes working with owners and operators of critical infrastructure to support cybersecurity preparedness through risk assessment, mitigation, and incident response capabilities and by securing unclassified networks for federal civilian departments and agencies, or what is called the “.gov domain” (DHS, 2011d).

The White House Cyberspace Policy Review laid a foundation for the scope, reliance, and interrelatedness of our technology and communications systems, and it called for the development of a cybersecurity incident response plan. To address this, CS&C developed the National Cyber Incident Response Plan (NCIRP) in accordance with the principals of the National Response Framework (NRF). The NCIRP describes how the nation responds to significant cyber incidents. (The NCIRP definition of a significant cyber incident is set out in Appendix A.) The NRF enables all response partners to prepare for and to provide a unified national response. The NCIRP defines a significant cyber incident and expands on the NRF to address the unique operational response structure.

The NCIRP was developed through numerous collaborative federal, state, local, and private sector interactions. The March 2011, interim version 1.8 of the NCIRP was

approved as an interim plan pending revision at the National Security Staff deputies' committee meeting on cybersecurity on August 27, 2011. The approval process included incorporation of the lessons learned from Cyber Storm III. In September 2010, Cyber Storm III tested the NCIRP.

Cyber Storm III is a DHS-sponsored exercise that brings together a diverse cross section of the nation's cyber incident responders to plan and assess U.S. cyberresponse capabilities. "Securing America's cyber infrastructure requires close coordination with our federal, state, international, and private sector partners," DHS Secretary Janet Napolitano said in a statement in regard to the Cyber Storm III exercise (DHS, October 4, 2010c).

The NCIRP sets the strategic direction for how the nation responds to cyber incidents and how operations are escalated into a nationally coordinated response for significant cyber incident activities. A significant cyber incident sets the conditions in the cyber domain that require increased national coordination. This increase in national coordination is triggered when the National Cyber Risk Alert Level (NCRAL) system is set at severe or critical. The NCRAL has a five-level system that starts with day-to-day operations designated as 1) normal, 2) guarded, 3) elevated, 4) severe, and 5) critical. This system takes into account the threats, vulnerabilities, and potential consequences across the cyberinfrastructure and provides an indication of the overall national cyberrisk. Each of the levels has associated risk and expected actions, as set forth in Appendix D.

C. PROBLEM STATEMENT

President Obama has stated: "No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge" (White House Office of the Press Secretary, 2009). The federal government cannot respond alone to secure cyberspace. Rather, the cyberspace ecosystem environment requires a national partnership that includes our state, local, tribal, and territorial governments and the private sector.

Information and communication technologies continue to evolve in cyberspace. To address growing threats and vulnerabilities, the national partners must be adaptive and must adjust in order to respond to cyber incidents more effectively and efficiently. This approach should include analysis and evaluation of the use of standard methods and terms, standardized notification and reporting, unified resource management, and the integration of information flow. All of this should lead to the optimization of the cyber incident response through the strength of a combined effort and the lessening of duplicative efforts. “Given this constantly changing landscape, we must continually assess the effectiveness of our prevention, protection, and response efforts in cyberspace and adjust the NCIRP and other strategic, operational, and tactical plans accordingly” (DHS-CS&C, 2011).

A cyber incident response can be a data hungry atmosphere, and an ad hoc approach to the issue without the use of standards and developed procedures could present unnecessary challenges. It can be problematic when developing courses of action for a cyber incident when the approach is not universally understood, accepted, and used by all those affected.

The DHS Quadrennial Homeland Security Review Report (QHSR) identifies the importance of what is referred to as the homeland security enterprise. The enterprise includes the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in cyberspace. The QHSR has five overarching mission areas: mission area four is the safeguarding and securing of cyberspace. The QHSR states, “We must invest in the innovative technologies, techniques, and procedures necessary to sustain a safe, secure, and resilient cyber environment” (DHS, 2010a). Sustaining a safe, secure, and resilient cyberecosystem should include documented standards and adaptive methods and procedures.

CS&C engaged extensively with cyberspace partners to build the NCIRP. It will continue to engage with them as that program grows to meet new challenges. With the constantly changing landscape of cyberspace, adjustments must be made to the NCIRP and other plans as required.

The NCIRP provides autonomy to states for cyber incident response and stipulates that, until amended, the contact point for a significant cyber incident is the state homeland security advisor (HSA). The state HSA serves as counsel to the governor on homeland security issues and may serve as a liaison between the governor's office, the state homeland security structure and the DHS. Currently the NCIRP does not have a documented response procedure or operational construct, risk model, or alerting and notification methodology that could standardize states' support to a significant cyber incident beyond contacting the HSA.

D. TENTATIVE SOLUTIONS

1. Summary

Significant cyber incident response solutions should include recognized, standardized, and documented plans and procedures for cyberspace incident constructs, risk models, or notification and alerting methodologies. This will enable the effective and repeatable transfer of intent, objectives, resource limitations, and desired outcome for a cyber incident. The roles and responsibilities associated with the intent, objective, and outcome for a cyberspace incident should be understood and documented, as well as allowing for preincident preparatory planning. The preparedness, response, and recovery of states for a cyber incident or event will be variable, both in their inherent knowledge and in their capabilities. The use of centers, hubs, or nodes for information distribution and resource management could address limited cyber incident response capabilities and encourage the likelihood of obtaining desired outcomes.

2. Coordinated Alerts, Notifications, and Risk Indexing

The NCRIP explains how a significant cyber incident is triggered by an increase in the risk indexing system, NCRAL. The NCRAL system enables an evaluation of risk to the information and communication technologies that support the nation's security. It examines threats, vulnerabilities, and consequences. It does not use a color-coded system as it moves through its index categories of day-to-day to critical.

Color-coded systems should be reviewed. Color-coded alerting methodologies—such as those used by DHS—can be confusing and misunderstood if the community they alert is not familiar with each of the color categories or if the alert remains indefinitely at one color. To address potential confusion associated with color-coded alerting methodologies, research will review risk indexing tools like the NCRAL system to alert the states of a cyber incident that is not color coded. An example of the challenges associated with color-coded alerting methodologies is the replacement of the DHS color coded Homeland Security Advisory System (HSAS), which was initiated in 2002. In April 2011, the HSAS was officially replaced with the National Terrorism Advisory System (NTAS). The new NTAS removed the color-coded risk indexing scheme. It is believed the NTAS will more effectively communicate information about terrorist threats by providing timely detailed information about the event—and not just a change in color.

3. Coordinated Organizations

The use of centralized or regional centers, hubs, or nodes for incident coordination, information distribution, and resource management could address capability shortfalls. The NCIRP points to the National Cybersecurity and Communications Integration Center (NCCIC) for a significant cyber incident where it would coordinate national response efforts. The NCCIC works directly with federal, state, local, tribal, and territorial governments and private sector partners (DHS-CS&C, 2011).

The NCCIC is a 24x7operational element of CS&C for the production of a common operating picture for cybersecurity and communications across the federal, state, and local government, intelligence and law enforcement communities, and the private sector (DHS, August 9, 2011c). When Secretary Napolitano opened the NCCIC, she stated, “Securing America’s cyber infrastructure requires a coordinated and flexible system to detect threats and communicate protective measures to our federal, state, local, and private sector partners and the public” and “consolidating our cyber and communications operations centers within the NCCIC will enhance our ability to effectively mitigate risks and respond to threats” (DHS, 2009b).

Another centralized or regional center for the notification of a significant cyber incident could be the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC is viewed as the focal point for cyberthreat prevention, protection, response and recovery for the nation's state, local, territorial, and tribal governments (Multi-State Information Sharing and Analysis Center [MS-ISAC], 2011).

The NCIRP maintains that the MS-ISAC should be seen as a key resource for state, local, tribal, and territorial government information sharing; early warnings and alerts; mitigation strategies; training; exercises; and maintenance of overall cybersituational awareness (DHS-CS&C, 2011). Much like the NCCIC, the MS-ISAC has a twenty-four-hour watch and warning cybersecurity operations center, which was launched with the White House cybersecurity coordinator, Howard Schmidt, present. From the viewpoint of the MS-ISAC, the cybersecurity operations center builds on a long-standing information sharing partnership between the DHS, with an expectation of enhancing situational awareness at the state and local levels for the NCCIC (DHS, 2010b).

Under the authority of Department of Homeland Security Appropriations Act of 2010, Title III, the catalog of federal domestic assistance states that the DHS obligated an estimated $3,000,000 in fiscal year 2010 to the MS-ISAC. The type of assistance is a cooperative agreement with the objective of supporting activities involving cybersecurity protections for state, tribal, and local governments (Catalog of Federal Domestic Assistance, 2011).

Due to the autonomy of the states guaranteed by the Declaration of Independence and the disparate cyberspace capabilities and methods that the states employ, it is prudent to understand these and other processes as they pertains to this research before a significant cyber event.

E. LITERATURE REVIEW

1. Summary

This review identified pertinent literature that provided insight and guidance to those standardized operational cyberspace event models that could support states in a significant cyber incident, as defined by the NCIRP. The literature review examined the value, feasibility, and merit of other event and incident alerts, emergency notification models, and risk assessment mythologies.

The review analyzes common threads in other incident declarations or notification systems and risk models, including the cyberspace system, e.g., the Maritime Operational Threat Response, Amber Alert, the Emergency Alert System, the Integrated Public Alert and Warning System, the World Health Organization's pandemic alert, the electricity sector's physical security measures, and the cyberspace ecosystem. Analysis and evaluation of other similar models had common and useful factors for the thesis research inquiry into those standardized operational cyberspace event models that could support the states during a cyber event.

2. Notifications and Alerts

During the State of the Coast Guard address in March of 2009, the then-Commandant of the Coast Guard, Admiral Thad Allen, spoke of a process known as the Maritime Operational Threat Response, or MOTR. Using the 2004 national strategy for maritime security as a catalyst, the MOTR has matured over the years as an interagency notification tool. Utilizing prearranged protocols, federal officials coordinate their efforts to identify and mitigate risk in the maritime domain. During his speech Admiral Allen said, "The MOTR process is a gold standard for interagency coordination and cooperation," adding that "this is an unequivocal interagency success story" (United States Coast Guard, 2009).

The MOTR notification process includes numerous federal agencies, much like the model that this research sought, that provide a collaborative environment to develop

courses of action in response to threats through their command centers and designated experts. The MOTR process allows the contributing agencies to supply their knowledge, experience, and capabilities to address the threat in the maritime domain (Kreisher, 2009). Much like the cyberspace domain, the utilization of MOTR in the maritime domain requires a broad, collaborative approach to ensure that the desired outcome is fully discussed and fully informed by all the agencies that have a stake in that outcome.

Policy guidelines to enhance national and homeland security in the maritime domain are addressed by National Security Presidential Directive 41 (NSPD-41) / Homeland Security Presidential Directive 13 (HSPD-13). A key element of the nation's maritime security policy is the national strategy for maritime security, which defines the maritime domain as a system that—much like cyberspace—touches many areas of federal departments and agencies, state and local governments, the private sector, and international organizations (White House, 2005, p. 1).

The MOTR provides a coordinated response to threats against the United States and its interests in the maritime domain. The network of integrated agencies utilized during the MOTR provides a platform for national-level interactions for a coordinated, unified, timely, and effective information flow, in support of MOTR execution (United States Joint Forces Command, 2011). Furthermore the DHS is the lead MOTR agency, thus providing another potential link to its viability to state models for cyber incidents. Review of the MOTR notification methodology was beneficial to the research and evaluation for models applicable to state methods for cyber incidents.

Evaluation of existing matured and seasoned alert systems and processes was helpful for the research as well. One alert system that has proven itself numerous times is the Amber Alert. Amber Alerts use technology to disseminate information about child abductions in a timely manner (Library of Congress, 2009, p. 1). The Amber Alert uses an existing system called the Emergency Alert System (EAS). EAS sends emergency messages with the cooperation of broadcast radio and television and most cable television stations. Its most common use is for weather alerts (Library of Congress, 2009, p. 2). The Amber Alert leverages existing systems—an important aspect of this research due to the varying degree of capabilities of the states as they address cyber incidents. Understanding

how other alert models utilize existing systems was invaluable in the research of standardized operational cyberspace event models. Amber Alert plans are partnerships that include law enforcement agencies, highway departments, and communication companies that provide emergency alerts (Library of Congress, 2009, p. 1). A state's response and recovery for a significant cyber incident is also a partnered and collaborative event. Review of the Amber Alert process demonstrated a successful and currently deployed alert system to benchmark and learn from.

Another alert and notification system that gave instructive guidance was the EAS, mentioned above. The Federal Emergency Management Agency (FEMA) jointly administers the EAS with the Federal Communications Commission (FCC), in cooperation with the National Weather Service (NWS), an organization within the National Oceanic and Atmospheric Administration (NOAA). The EAS is built on a structure conceived in the 1950s but now refurbished with new technologies to bring the system up to twenty-first-century standards (Library of Congress, 2010). As part of the refurbishments, FEMA is developing the Integrated Public Alert and Warning System (IPAWS) to meet requirements for the new alert system. IPAWS was specified by an executive order (EO) issued by President George W. Bush in 2006 (Library of Congress, 2010, p. 8). This analysis gives helpful data on a few fronts: 1) It is a collaborated national alert system; 2) it is meeting new demands established by current technologies; and 3) it is an example of a national endeavor as specified by the EO. A significant cyber incident that involves the states needs to be grounded in all three of these areas. Although IPAWS is embracing new technologies and is a national endeavor, the IPAWS program has fallen behind schedule. The Government Accountability Office attributed the lack of progress mainly to "shifting program goals, lack of continuity in planning, staff turnover, and poorly organized program information from which to make management decisions" (Library of Congress, 2010, p. 1). Ensuring a timely and effective state response for a significant cyber incident will require determined and executable planning; it must also take into account staff turnover due to political cycles; and it must have obtainable goals and outcomes.

Research regarding recent events led to informative data. In the last few years, H1N1 pandemic planning and preparedness was a the focus of a national and international declaration. The World Health Organization (WHO) provided a declaration as guidance about pandemic alert levels to the national and international community (University of Pittsburgh Medical Center, 2009). The WHO pandemic alert phases were initially outlined in its 2005 global influenza preparedness plan, but in April 2009 the WHO revised its pandemic plan and alert scale to reflect advances that had occurred since 2005. These advances included increases in the understanding of past pandemics and strengthened outbreak communications. Defining cybersecurity response based on the real or perceived vulnerabilities of cyberspace is currently very dynamic. The WHO transitional posture with the emerging expanse of the pandemic threat was also very dynamic. The fast-paced and daily emerging dynamic environment of the WHO guidance, which positioned the national and international communities for a prepared response, was beneficial for this research.

Review of specific examples was important, but observed or empirical data research was important as well. Alert analysis and situational awareness have become very important as information and communication technologies become increasingly widespread to emergency responders (International Community on Information Systems, 2010, p. 1). This paper investigated trends and patterns embedded in alert notifications generated over a given period of time in order to uncover correlations that may exist in the data. Study data was mined from the National Center for Crisis and Continuity Coordination (International Community on Information Systems, 2010, p. 2). This empirical data revealed that correlations in state responses to significant cyber incidents should be reviewed in order to understand common methods and terms, standard notification and reporting processes, unification of resource management, and the integration of information. The National Center study took place over a two-year period, with only one source of collection, which could constitute a bias in the data. A greater number of data collection points could resolve this weak point in their methodology and provide the necessary conclusive correlations and paths to consider. This research looked at the broadcast of large numbers of alerts that may impair the ability of analysts to

adequately make informed decisions in a timely fashion. A timely response with well-informed decision-making capability is a universal necessity for any declarations, alerts, and emergency notifications.

3. Risk Indexing

DHS has eighteen critical resource key infrastructure (CRKI) categories. Some of these categories utilize risk indexing mythologies. One of those, the electricity sector, uses physical security measures to be considered for a defined threat alert level. The North American Electric Reliability Council (NERC) uses a five-level color-coded system, in which level 1 is green (low); 2 blue (guarded); 3 yellow (elevated); 4 orange (high); and 5 red (severe). There are basic standards and procedures for a given level (North American Electric Reliability Council [NERC], 2002a, p. 3). As in the case of the Department of Homeland Security's homeland security threat advisories, which were replaced by the NTAS as discussed earlier, color coding can be misleading or confusing if the responder is not intimately aware of the definitions of each color. This is a consideration that could nullify any benefits that a simple color-coding approach could provide. Although a quantifiable element is helpful as levels are increased or decreased, consideration was based on how to convey a complex transition in a simple manner. Moreover, this report helped define the scope for measures that each organization can implement for its specific alert level response plans. Risk planning is a fundamental and critical area for declarations, alerts, and emergency notifications, regardless of type.

The electricity sector provided further guidance in the specific area of cyberresponse. This guide also gives examples of security measures to be considered on a given cyberthreat level, i.e., 1 green (low); 2 blue (guarded); 3 yellow (elevated); 4 orange (high); and 5 red (severe) (NERC, 2002b, p. 3). The fact that both NERC documents use the same color-code and naming conventions exposes a possible weakness. Models with like quantifiers can be problematic. Both a response guideline for an alert level and an accompanying definition is provided, which would be a prudent approach for a standardized operational cyberspace event model as well (NERC, 2002b, p. 2). The guidance is not an exhaustive list of possible security measures but its review

and analysis lead to more in-depth cyber response literature. Furthermore, this literature points out the fact that not all measures are applicable to all organizations—a reference to the unique capabilities found in each state.

Another area of risk mythology reviewed was threat-risk indexing. A threat-risk index can provide a quantitative variant or basis for either prioritizing security upgrades or updating the qualitative national color-coded threat alert (Idaho National Engineering and Environmental Laboratory, 2004). Although other risk-based approaches were considered, this particular report examined a quantitative approach employing scientific and engineering concepts to develop a threat-risk index for decision makers to utilize. Risk methodologies can provide delineations for courses of actions for all phases of a cyber event, i.e., preparedness, detection, analysis, response, and resolution of the event or incident.

During this research it was observed that many risk-based methodologies resemble or appear to be iteratively derived from W. Edwards Deming's continuous process feedback loop. In the 1950s, Deming proposed that a business process should be analyzed and measured to identify sources of variation that cause products to deviate from customer requirements. This cycle is commonly known as the PDCA cycle (or plan, do, check, act). The PDCA cycle feedback loop dictated the need to assess and measure effectiveness, which would be used as feedback for possible improvements.

Much like the PDCA cycle, the DHS National Infrastructure Protection Plan (NIPP) proposes a continuous feedback loop with its risk management framework (DHS, 2009a, p. 27). Both give process flow considerations that provide insight into procedure paths as to their relevance to a standardized operational cyberspace event model for a state cyber event.

4. Cyberspace Environment

During a speech made by DHS Secretary Janet Napolitano at the University of California Berkeley College of Engineering, she stated that cyberspace security requires a full range of partners and that DHS is currently building a technical ecosystem based on a

concept of cyberspace as a distributed space (DHS, 2011b). During the Berkeley speech, Napolitano deliberately used the term "ecosystem" to indicate that cyberspace is a dynamic, even organic environment that cannot be treated as self-contained. In the cyberspace security industry, partners have depicted this environment as an ecosystem.

This evaluation gives credence to the necessity to recognize that the cyberspace environment operates much like a cyberspace ecosystem (Booz Allen Hamilton, 2011). With its numerous interconnections and interdependencies among diverse stakeholders, networks, applications, systems, and computing devices, the health of one component can and frequently does impact the health of the ecosystem itself. It was important to comprehend this diversity of cyberspace its manifestation as an ecosystem that will require organizations to gather, filter, integrate, analyze, and comprehend vast amounts of information for a response.

F. METHODOLOGY

1. Method

Qualitative analysis of semistructured survey data, along with an extensive review collected from 19 states, was used to better understand how standardized operational cyberspace events are being defined and what risk models and alerting models are being used by the states. What common cyber events, risk models and alert protocols appear among states, and which of the aforementioned could support the states during a significant cyber incident as defined by the NCIRP?

2. Sample

Formal documented questions that pertained to cyber incident response were formulated and sent to state chief information officers, state chief information security officers, state homeland security officers, and other individuals who would be central to this mission area. The answers were returned and compiled for their relevance to this research. State chief information officers and state chief information security officers are on the front end of the cybersecurity dialogue, lending expertise to the identification of

gaps in policy and testing strategies for remediation in order to address threats in the states' evolving cybersecurity environment (Williams, 2009).

Technical and academic literature from the private and public sectors was reviewed. A common thread was found in documentation, technical and academic literature event models, and incident declarations or notification systems. Analysis and evaluation of other similar models had common and useful factors for this thesis research. The review included communities that utilize event and incident declarations, alerts and emergency notifications, and risk assessment mythologies. Moreover, empirical data research was important.

Other existing models were evaluated and applied where appropriate, e.g., the Emergency Alert System, which sends emergency messages with the cooperation of broadcast radio and television; the National Cyber Risk Alert Level system, which triggers national coordination for a significant cyber event; the North American Electric Reliability Council, which uses a five-level color-coded system; and pandemic alert level declarations to the national and international community by the World Health Organization.

A combination of states, some with a robust security posture some to with a lesser position, assisted in the development of an operational model for a significant cyber incident. Also important to the research was an understanding of key state contact points, interconnectivities, and resources, e.g., the state CIO, the state chief ISO, MS-ISAC; Communications ISAC; Information Technology ISAC; NCCIC, the National Operation Center (NOC); and the National Infrastructure Coordinating Center (NICC).

These organizations were useful to the research for the following reasons: The MS-ISAC is a collaborative state and local government–focused cybersecurity entity that addresses cyberthreat prevention, protection, and response and recovery throughout the states of our nation. The NCCIC combines two of DHS's operational organizations: the National Coordinating Center (NCC) for Telecommunications and the United States Computer Emergency Readiness Team (US-CERT). The NCC is the operational arm of the National Communications System. It provides a mechanism to coordinate the

initiation and restoration of national security and emergency preparedness telecommunication services in times of crisis. It is a joint industry- and government-staffed center to handle emergency telecommunication requests. The US-CERT's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aid to national recovery efforts for critical infrastructure information systems. The NOC serves as the primary national-level hub for domestic situational awareness, common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management. Finally, the NICC serves as the DHS Office of Infrastructure Protection's focal point for coordination with the eighteen national critical infrastructure and key resources sectors during steady-state operations and during incident management activities.

3. Data Collection

In order to formulate a standardized operational cyberspace event, risk model, or alerting methodology, written questions were posed to the states in addition to phone and in-person interviews to obtain original data. Formal documented questions were formulated that had their bases in NCIRP, internal and external CS&C interactions and protocol, and personal experience. Initially my Naval Postgraduate School (NPS) colleagues at the state and local level were asked to introduce the researcher via e-mail to state points of contact who support the cyberspace mission area, i.e., the state chief information officer, the state chief information security officer, the state homeland security officer, and other individuals who would be key state players.

A total of 31 states were contacted through these introductions to cyberspace incident response points-of-contact by NPS colleagues, other cyberspace incident response points-of-contact through the state contacts, state interactions at Cyber Storm III, public Internet searches, and cold calls. Most initial contacts were made through e-mail over a five-month period. I received 19 responses. Six of the states did not respond to my inquiry, five were not able to answer the questions for various reasons, and one state thought the communication was a phishing e-mail and answered with the

notification that “this person has attempted to contact me multiple times but I have chosen to ignore his request due to the nature of the questions he has asked.”

All interaction with the states was personalized, i.e., e-mails were addressed to that state and the cyberspace point-of-contact (POC); the questions included that particular state’s POC and their state flag. The following is indicative of the email message sent:

> I would like to ask if you or your staff would participate in my research study entitled “State Methods for a Cyber Incident” on a voluntary and confidential base. This research is an academic thesis study for my Master of Arts in Security Studies (Homeland Security and Defense) for the Naval Post Graduate School. I have 10 questions I would like to provide to you to get input from the State of Delaware as it relates to cyber events. I believe this research could help shape a cyber response at the State and Federal level.
>
> I appreciate any assistance that you could provide with these questions. In addition if you could e-introduce me to your colleagues in other States that would be extremely helpful.
>
> Please contact me at this email or the phone numbers below with any questions.

Once the POC responded, I sent the following e-mail message with the questions attached:

> Please find the questions in the attached. For planning proposes I will need to set a date of 28 April 11 when I hope you can provide your answers. If this does not meet your schedule please let me know a better date for you. Due to research data integrity please don’t send this form or the questions beyond the State Government Offices you represent.
>
> I appreciate any assistance that you could provide with these questions. In addition if you could e-introduce me to your colleagues in other States that would be extremely helpful.

4. Data Analysis

In seeking to better understand state standardized operational cyberspace events, 19 states were analyzed by survey question rather than by state. The research evaluated possible commonalities, identified variance among them, and reviewed the models being used by the states. The data analysis process was performed as follows: 1) Each survey was coded, looking for particular phrases that describe particular state practices, processes, and/or status; 2) all practices, processes, and/or status were grouped by research questions using a table format. Once key phrases were organized by research question, the researcher used open and axial coding to assist in locating commonalities and patterns in the data, while at the same time taking note of the level of variance among the states.

As discussed previously, a total of 31 states were contacted over a five-month period. Of those 31 contacted, 19 (61 percent) responded. Initially, there were 10 original questions, but 13 questions were posed to the states. Questions 3a, 3b, and 3c were added after some of the state responses were received, due to knowledge gleaned from the input of the states. A total of 227 answers were received.

The following questions were given to the states. The questions were asked with the anticipation that the states would have a basic knowledge of the NCIRP and its definition of a significant cyber incident.

Table 1. Questions Given to the States

Count	Question
1	How does your State define a State Cyber Incident?
2	Who is the key State individual that would be contacted for a State Cyber Incident?
3	What Office/Department/Section does that key State individual work for that would be contacted for State Cyber Incident?
3a	How are reports gathered for a State Cyber Incident?
3b	Is there a requirement that State Cyber Incident be reported?
3c	What level of involvement was your State engaged, with the coordination of the development of the DHS National Cyber Incident Response Plan (NCIRP)?
4	How does your State define a National Significant Cyber Incident?
5	Who is the key State individual that would be contacted for a National Significant Cyber Incident?
6	What Office/Department/Section does that key State individual work for that would be contacted for National Significant Cyber Incident?
7	What alerting methodologies or procedures do your State use for a Cyber Incident notification?
8	What is a predominant cause of a State Cyber Incident? • Insider—Person motivated by revenge, greed, conducts malicious or hostile activities in cyberspace. • Hacktivist—Utilizes technology to announce a social, ideological, religious, or political message. • Cyber Criminal—Uses malware and exploits to steal goods, money, identities, or passwords. • Individual Hacker—Breaks into cyberspace and networks motivated by the challenge to prove their skills, brag to friends, and are thrilled to engage in unauthorized activities. • Industrial and Technology Espionage—Collection of science, intellectual property, or technology information that could provide economic or strategic benefits. • Terrorism—Connecting—Propaganda, fund raising, recruitment/radicalization. • Terrorism—Cultivating—Operational and planning communications, funds transferred, training in cyberspace. • Terrorism—Exploiting—Cyber attacks against targets. • Other—Explain.

Count	Question
9	How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.
10	How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.

II. ANALYSIS

The following are general observations from each of the questions posed to the states. A complete listing of all the questions asked of the states and their responses is found in Appendixes B. Detailed patterns and interpretations of the research data are found in the next chapter.

A. QUESTION 1: DEFINITION OF STATE CYBER INCIDENT

Question 1 was posed as "How does your state define a state cyber incident?"

State responses included terms like "activity," "incident," and "event," indicating a change in recognized day-to-day operations to an accelerated operational stance. In addition, the data showed that some states opted to define a state cyber event with concise statements that included phrases showing the detection of a known threat or vulnerability, e.g., "infection or unauthorized access;" "exposure of sensitive information;" "unexplained network or system behavior;" "a breach of the data confidentiality;" and "compromise of the confidentiality, integrity, or availability of data and information technology resources." Furthermore, various states answered the question by directing the researcher to state-recognized and established security policies, standards, and procedures.

One of the states made a distinction between a "cyber incident" and an "information security incident," making the point by stating that an information security incident can also involve paper or people, not just technology.

Lastly, one state embraced a federal agency definition found in the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Information Security Glossary of Key Information Security Terms. This particular state also built much of its plans, policies, and procedures on other NIST documents, e.g., the Computer Security Incident Handling Guide (United States Department of Commerce, 2008).

B. QUESTION 2: KEY CONTACT FOR STATE CYBER INCIDENT

Question 2 asked, "Who is the key state individual that would be contacted for a state cyber incident?"

Historically, certain organizations have been established that have recognize the significance of state CIOs, including the National Association of State Chief Information Officers (NASCIO), an association that represents state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. States have also seen the necessity of integrating cybersecurity into overall state infrastructure planning. "The state-level CISO stands in the middle of these large and complex issues, serving as the partner of the CIO in ensuring the protection of state data and systems" (IBM Center for the Business of Government, 2010).

In most instances, the answers to Question 2 showed that the state CISO is the key state individual contacted for a state cyber incident. One of the other titles of those contacted was a variation of the state CISO, i.e., information security and privacy officer. Two of the states used an incident response team, and the teams operate within the construct of the offices of the CIO or CISO.

C. QUESTION 3: KEY DEPARTMENT FOR STATE CYBER INCIDENT

Question 3 asked, "What office/department/section does that key state individual work for that would be contacted for state cyber incident?

Many of the states use offices with "security," "technology," "information," or "enterprise" in the title. The predominate word, as expected, is "security." Three of the states house the offices within their department of administration. One of the states has linked its information security with its privacy office.

D. QUESTION 3A: REPORT GATHERING FOR STATE CYBER INCIDENT

Question 3A was posed as: "How are reports gathered for a state cyber incident?"

One state relies on analog methods, i.e., verbal reports. Secure web tools, customizable tracking and log applications that employ recognized incident reporting forms, ticketing reporting systems, help desks and hotlines, are included in the methods that the states utilize.

E. QUESTION 3B: REPORTING REQUIREMENT FOR STATE CYBER INCIDENT

Question 3B asked, "Is there a requirement that state cyber incidents be reported?"

The States that responded to this question said that they did have a requirement to report a state cyber incident; in some cases that requirement is legislated by the state. One state noted that the state executive branch is required to report but that some of the institutes—for example higher education—are not. One state noted that it can take systems offline if deemed necessary.

F. QUESTION 3C: INVOLVEMENT WITH NCIRP

Question 3C inquired, "What level of involvement was your state engaged with the coordination of the development of the DHS National Cyber Incident Response Plan (NCIRP)?"

Review of the responses showed that the states had varying degree of involvement, from "none at all," "not sure," "minimal," and "not directly, but through MS-ISAC and the National Association of State Chief Information Officers Security and Privacy work group."

G. QUESTION 4: STATE DEFINITION OF NATIONAL CYBER INCIDENT

Question 4 asked, "How does your state define a national significant cyber incident?"

Many states responded that they did not have a definition or would not be the entity to define that. One state acknowledged the complexity of making such a determination, but those that did provide a brief answer agreed that the incident would be one that exceeded state capabilities or overwhelmed state government and industry, i.e., it affected multiple states or regions or impacted critical infrastructure, national process, or economy. Lastly, one state used the definition inherent in the NCIRP, i.e., when the NCRAL system is set at "severe" or "critical."

H. QUESTION 5: KEY CONTACT FOR NATIONAL CYBER INCIDENT

Question 5 queried, "Who is the key state individual that would be contacted for a national significant cyber incident?"

The answers to this question were similar to the contacts given in response to Question 1 regarding a state cyber incident. One underlying theme in this answer was an elevated leadership notification all the way to senior officials in the state, e.g., the governor or the governor's homeland security advisor. One state stipulated that it would contact the state infrastructure protection center, which is supported 24 hours a day. The infrastructure protection center would also coordinate with the network operation center, the security operation center, and the privacy office. Having a 24-hour operational element within the state's own funding and management control indicates a strong commitment to the cyberspace mission area.

I. QUESTION 6: KEY DEPARTMENT FOR NATIONAL CYBER INCIDENT

Question 6 asked, "What office/department/section does that key state individual work for that would be contacted for a national significant cyber incident?"

The answers to this question were similar to given in response to Question 3, concerning a state incident.

J. QUESTION 7: STATE CYBER INCIDENT ALERTING METHODOLOGIES

Question 7 inquired, "What alerting methodologies or procedures does your state use for a cyber incident notification?"

This question was one of the fundamental questions presented to the state. It was formulated with the expectation of eliciting responses with direct implications for the research question.

E-mails, text messages, emergency and alert notification systems, web-based tools, and formalized and published incident plans were recognized as methods.

K. QUESTION 8: PREDOMINANT CAUSE OF STATE CYBER INCIDENT

Question 8 asked, "What is a predominant cause of a state cyber incident?"

The predominant cause of a state cyber incident, according to the greater numbers and the content of the states' answers, was "cyber criminals." Additional information for this cause included the qualifying language that the perpetrator "uses malware and exploits to steal goods, money, identities, or passwords." The next most predominant cause given was "individual hacker," with the qualifying definition that the perpetrator "breaks into cyberspace and networks motivated by the challenge to prove their skills, brag to friends, and are thrilled to engage in unauthorized activities."

L. QUESTION 9: CURRENT RESPONSE TO STATE CYBER INCIDENT

Question 9 asked, “How does your state currently respond to a state cyber incident?”

The predominant answer to this question was the utilization of the state operation center. A principal information-sharing and analysis center brought into play was the Multi-State (MS-ISAC).

M. QUESTION 10: STATE RESPONSE TO NATIONAL CYBER INCIDENT

Question 10 was posed as “How would your state respond to a national significant cyber incident?”

The answers to this question were similar to given to Question 9, i.e., responding to a state cyber incident is viewed as very similar to responding to a national significant cyber incident.

III. FINDINGS AND INTERPRETATIONS

The following describes the detailed patterns and the interpretations of the answers provided by the states for each survey question. Due to the sensitivity of the data the state will only be referenced with an identifier key. As can be ascertained from Appendix B, State Response to Questions, some states submitted their policy and standards or the state web page where similar data could be found. The approach will focus on the explicit answers given, rather than an extensive review of the state's policy and standards. At the end of each question, key patterns and interpretations will be provided. A summary of all the patterns and interpretations of the answers provided by the states for each survey question is provided at the end of this section.

It is recommended that future research consider a comparative analysis of state cyber policy and standards as they relate to the overall security mission area that resides in cyberspace and that impacts an extremely diverse community of users and their wide range of needs. Furthermore, the analysis of state cyber policy and standards could add to the operational cyberspace event, risk models, or alerting methodologies found in this research for a significant cyber incident.

A. QUESTION 1: DEFINITION OF STATE CYBER INCIDENT

1. Findings

The state definition of a state cyber incident presented a diverse spectrum of understanding, approaches, and terms. In a national-level event or a large incident that encompasses multiple states, a common understanding by varied groups, agencies, or departments regarding how to plan for, respond to, or recover from the event can be very important in a time-dependant situation. Furthermore, common approaches and terms is also beneficial when dealing with the complex system that resides in cyberspace.

Using recognized and established definitions—as in the case of State N-14's use of the NIST Information Security Glossary of Key Information Security Terms and State E-5's use of the NIST Computer Security Incident Handling Guide—shows the willingness of states to utilize federal plans, policies, and procedures.

As discussed in Appendix A, the NCIRP definition denotes that a significant cyber incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. The use of "confidentiality, integrity, or availability" is also seen in other federal documents (United States Department of Commerce, 2008, p. 5-1). States F-6, H-8, I-9, J-10, N-14, O-15, and S-19 all used some form of this language or explicitly stated the terms "confidentiality, integrity, or availability." Universally recognized terms like these for the federal, state, local, and industry cyberspace community could be established—which at a foundational level gives a common starting point. Differences in cyberspace security terms can be small or subtle, as in the areas of approach to the subject, the methodologies used, and the areas of concentration, but ultimately the differences can have hugely differing responses.

State P-16 made a distinction between a "cyber incident" and an "information security incident," making the point that an information security incident can also involve paper or people, not just technology. The NCIRP definition of a significant cyber incident expands upon and includes the destroying, degrading, or disrupting of the cyber infrastructure and/or the integrity of the information that supports the private and public sectors. This "supporting" comment could be inferred to encompass paper or people, but explicit language is important in the technical, distributed, and diverging needs found in the cyberspace ecosystem.

Lastly, State P-16 rank-ordered areas because major risks to the state include the financial impact of a personal identifiable information (PII) breach and subsequent impact to state reputation. This state prioritizes incidents that result in an intentional or accidental PII breach.

2. Key Patterns and Interpretations

a. Common Terms

The use of universally recognized and established definitions and terms for the federal, state, local, and industry cyberspace community could be beneficial to the response to cyber incidents. The use of a common approach is not foreign to incident management. An incident-management system known as the Incident Command System[1] (ISC), which has its roots in wildfire management, has established itself as a foundational tool in creating a cohesive incident response. For example, this system was used during the response to the 9/11 terrorist attack at the Pentagon in Arlington, Virginia.

b. Risk-Based Methods

A risk-based approach to an incident can provide a systematic, aggregated, and rigorous analysis methodology. Risk-based ranking for complex systems can be a methodology that allows both those providing the data and those using the data to make operational and strategic paths toward judgments clearer, due to its indexing or hierarchical methods. Risk and its management can allow the identification, analysis, and communication of the incident risk.[2] This can permit decisions to be made to accept, avoid, transfer, or control the cyber incident to an acceptable level, considering the associated costs and benefits of any actions taken.

[1] The Incident Command System (ICS) is a recognized and standardized on-scene incident management approach that enables a coordinated response among various jurisdictions and functional agencies, using common terminology, processes, and organizational structure.

[2] DHS Risk Lexicon defines “risk” as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

B. QUESTION 2: KEY CONTACT FOR STATE CYBER INCIDENT

1. Findings

Key to the answers from this question is the desire to have the responsibility for a state cyber incident reside with the chief information security officer. The states (B-2, C-3, E-5, H-8, I-9, K-11, L-12, M-13, Q-17, R-18, and S-19) saw this, as a unique type of incident that necessitated an individual designated to address it.

States N-14 and P-16 used incident response teams, but the teams operated within the construct of the offices of the CIO or CISO. An approach that would utilize well-trained and accessible teams of subject matter experts does provide a cadre of quick response personnel, but funding a 24-hour operation could be costly and could necessitate an on-call rotation status. State N-14 uses an on-call approach along with the title of incident commander for the leader of their incident response team. As with any on-call or 24-hour personnel, it is important to establish documented expectations and guidelines in the area of pay, overtime, and estimated length of hours for response and recovery.

2. Key Patterns and Interpretations

a. Progression of Responsibility for Coordination and Control

For any incident, it is important to establish who is in charge, e.g., the chief information officer or the chief information security officer. ICS uses the position and naming convention of incident commander for the individual.[3] Inasmuch as ICS is a practice that has consistently shown a desired result, it is not a practice that should be overlooked for other areas of analogous connections.

[3] The incident commander is the incident command system organizational element responsible for overall management of the incident.

b. Specialized Teams

A specialized team like an incident response team could be deployed by the individual in charge and used on an as-needed basis. Law enforcement uses special weapons and tactics teams (SWAT) for exceptional situations that require increased firepower or specialized tactics. One of the divisions in CS&C is the National Cyber Security Division (NCSD). The DHS Control Systems Security Program (CSSP), operated under the NCSD, manages and operates the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the US-CERT. ICS-CERT is a specialized incident-response that which provides focused operational capabilities for the defense of control system environments against emerging cyber threats by responding to and analyzing control systems–related incidents.

C. QUESTION 3: KEY DEPARTMENT FOR STATE CYBER INCIDENT

1. Findings

State H-8 noted that the responsible office was the Office of Information Security, housed within the Governor and Cabinet Agency. According to State H-8, this responsibility for state cyber incidents was established by state law. This level of senior leadership could accelerate decision making for cyber events. This should come with the operational caveat that senior leaders cannot possibly be the subject matter expert for all scenarios and generally must rely on the team around them to make those decisions based on information from their subject matter experts.

Having roles and responsibilities defined and established by statute can be an important step in cybersecurity plans, policies, and procedures and be a compelling reason to comply. At the federal level, many reports have been written directed to the very issue of defining roles and responsibilities for cybersecurity (United States Government Accountability Office [GAO], 2010a; GAO, 2010b).

State D-4 has linked its offices and individuals to be contacted for state cyber incidents with its privacy office. Only State D-4 responded in this manner. Privacy issues

are in the forefront in many cyberspace dialogues. The E-Government Act of 2002 recognized that the availability of information, from personal information to public information, has important ramifications for the protection of personal information contained in government records and systems. The E-Government Act mandates an assessment of the privacy impact of any substantially revised or new information technology system. The document that results from these mandated assessments is called a privacy impact assessment (PIA). Like State D-4, the federal government recognizes the importance of privacy and of linking the state cyber office directly with the privacy office. This combination of linking offices and individuals to be contacted for state cyber incidents with their privacy office could ensure the protection of personal and public information through real and perceived scrutiny.

Finally, if a state cyber incident is confined within its own geographic borders, it could be less important to not put an emphasis on common titles. A cyber incident—whether on a national, state, or local scale—is frequently not confined by borders. This factor of crossing borders is not unique to a cyber incident of any scale. Common titles could be beneficial to expedite cyber incident response and recovery, whether within or outside the state's borders.

2. Key Patterns and Interpretations

a. Cyber Legislation

Many times government laws need to be passed not only to establish particular statutes but to allow the process of law making to take place. The diverse cyberspace community and its interconnected and interdependent ecosystem requires many critical voices to be heard. These many voices require a process, and the making of law can lend itself to that process and institute it for use and updates.

b. Roles and Responsibilities

Cyber incident management, like any management process, requires defined roles and responsibilities. Cyber legislation can support the defining process and

again bring to the table those who have a vested interest in the cyberspace mission space. As roles and responsibilities are being worked for senior leadership, it is important to build collaborative information sharing and flow processes simultaneously with the defining of the roles and responsibilities of the operational staff. Moreover, in the defining process a firm understanding is needed of all the players important to the security of cyberspace; this could include the privacy office, public affairs, acquisition, and apportions.

D. QUESTION 3A: REPORT GATHERING FOR STATE CYBER INCIDENT

1. Findings

Question 3a was added to the list of questions after some states had already responded to the original questions; therefore 12 of the total 19 states provided answers to 3a. The new questions were introduced after the original 10 questions due to input from subject matter experts at the Naval Postgraduate School and interactions with state CISOs.

States C-3 and P-16 use analog verbal reports that include regular updates and an initial report by telephone respectively. State L-12 does not have a formalized process, its approach being ad hoc. It is reassuring in pre- and post-incident management to have a person to talk to, but with the type of information, which could include video and data, and the volume that our nation's response groups have become accustomed to, relying on verbal reports alone could be problematic. The same reasoning applies to an ad hoc approach. Without standard procedures in an information- and data-hungry incident response atmosphere, an ad hoc approach could present unnecessary challenges.

State D-4 uses a secure incident management web portal; State E-5 uses an open online customizable application; State Q-17 uses a state portal; and State R-18 uses an online report form. States M-13 and O-15 are in the process of creating an Internet-based reporting tool or portal. State F-6 utilizes an incident-management help desk, and State J-10 uses a ticketing reporting system.

2. Key Patterns and Interpretations

Incident Management Support Tools: Secure username and password-protected portals or web-based tools that allow customizable tracking and log applications that employ recognized incident reporting forms, ticketing reporting systems, help desks and hotlines are all expedient methods in a time of crisis. Allowing access to these tools through Internet user name– and password-protected sites gives accessibility via any online connection or hot spot.[4] Some beneficial attributes of incident-management web tools are web conferencing; 24X7 availability; document and form libraries; geographical visualization; and a common operational picture. DHS utilizes the Homeland Security Information Network (HSIN), which is a national secure and trusted web-based portal for information sharing and collaboration.

E. QUESTION 3B: REPORTING REQUIREMENT FOR STATE CYBER INCIDENT

1. Findings

Question 3b was added to the list of questions after some states had already responded to the original questions; therefore 12 of the total 19 states provided answers to Question 3b.

All 12 states indicated that they did have a requirement to report a state cyber incident. States D-4, E-5, F-6, P-16, and R-18 all stated that they are mandated by legislation to report a state cyber incident. State O-15 stated that a recently passed law requires it.

As noted above, having legislated roles, responsibilities—and in this case notifications—defined and established can be a compelling reason to comply. On May 12, 2011, the White House introduced notification legislation (Executive Office of

[4] A hotspot is a site that offers Internet access over a wireless local area network through the use of a router connected to a link to an Internet service provider. Hotspots may be found in coffee shops and various other public establishments.

the President, 2011a). The legislation discusses Federal and State responsibilities for customer notification requirements for certain business entities (Executive Office of the President, 2011b).

State R-18 noted that the state executive branch is required to report but that higher education institutes are not required. This could pose challenges to managing a state cyber incident if all organizations do not follow the same reporting requirements.

State E-5 noted that it can take systems offline if deemed necessary. At the federal level, this one fact, the Internet on-off switch, has become very polarizing and is a very contentious area for any legislated cyberspace policy.

2. Key Patterns and Interpretations

a. Standardized Notification and Reporting

In developing courses of action for a cyber incident, it can be very problematic when the notification and reporting process is not universally accepted and used by all those affected.

b. Authority to Disconnect

The ability to disconnect noncompliant agencies from statewide networks due to a cyber incident that is impairing the confidentiality, integrity, or availability of that network is a compelling method for addressing threats and vulnerabilities. Disconnecting networks is a means to isolating systems. Disconnecting networks is a measure that should be well understood, and any cascading or indistinct associations should be well thought through before networks are disconnected. The management of the media and the information to be conveyed to the public are also aspects of the situation that should be brought to bear in this discussion as well.

F. QUESTION 3C: INVOLVEMENT WITH NCIRP

1. Findings

Question 3c was the last of those added to the list of questions after some states had already responded to the original questions; therefore, 15 of the total 19 states provided answers to Question 3c.

National-level documents, which include multistakeholders and diverse requirements from each community, can be very challenging to create, collaborate, and vet for universal acceptance. The NCIRP was no exception. With an understanding of the magnitude of the cyberspace mission and its security, DHS CS&C developed the NCIRP through numerous collaborative federal, state, local, and private-sector interactions. Based on NCIRP collaboration meeting documents, seven states were involved with its development. Those seven states were either not provided with research questions or were not able to participate.

A review of the answers showed that states had varying degrees of involvement. States B-2, E-5, M-13, and P-16 stated that they had no involvement. State H-8 said that it had minimal involvement and indicated that it would have been more involved if given the opportunity. State A-1 said that it saw its involvement in the DHS Cyber Storm III through the MS-ISAC, where the NCIRP was exercised, as involvement in the NCIRP development. State A-1 said that it did not have the funding to participate directly in the Cyber Storm III exercise through its representatives. Additionally, State A-1 stated that it had participated in a statewide cybersecurity tabletop exercise sponsored by its emergency management agency, which had been produced under the advice of DHS and FEMA. The purpose of the cybersecurity tabletop exercise was to provide participants with an opportunity to evaluate current concepts, plans, and capabilities for a response to a cyberattack against the state's computer networks and systems. The exercise was modeled after the Homeland Security Exercise and Evaluation Program (HSEEP). Multiple local, state, and government entities were involved in the exercise, which included border state representatives.

A means to stay involved with the potential of leveraging other insights and lower expenses can be realized through established organizations like the NASCIO. State Q-17 provided input to the NCIRP through the NASCIO Security and Privacy work group forum.

Finally, State I-9 recognized the challenges in its own organization: the state was given the opportunity to review for comments, but the document sat on the desk of another state department, which prevented others from having enough time to comment.

As stated above, national policies can be very challenging to create, collaborate, and vet for concurrence. The president has recognized that no single official oversees cybersecurity policy across the federal government and no single agency has the responsibility (White House Office of the Press Secretary, 2009).

The NCIRP, like other policies, requires stakeholders with vested interests to be involved with development and updates. DHS should continue its collaborative development of the NCIRP with the states and others that have vested interests in the response to a national significant cyber incident.

2. Key Patterns and Interpretations

a. Exercise for Proficiency

Exercises provide opportunities for departments and agencies to demonstrate competencies and strengths and to incorporate them in order to sustain and enhance their existing capabilities. Furthermore, exercises provide an objective assessment and evaluation of gaps and shortfalls in plans, policies, and procedures so that areas for improvement can be addressed prior to local or national cyber incidents. Exercises help to clarify roles and responsibilities among different entities and to improve combined interagency capability and interoperability.

b. Leverage Existing Organizations

Many capable and proven organizations exist that allow departments, agencies, the private sector, academia, professionals, and individuals to contribute their subject matter expertise and to glean information from other subject matter experts. A few of these organizations are the Anti-Virus Information Exchange Network (AVIEN); Applied Computer Security Associates (ACSE); the Forum of Incident Response and Security Teams (FIRST); the Government Forum of Incident Response and Security Teams (GFIRST); the International Association for Computer Systems Security, Inc. (IACSS); the Meridian Conference; the Multi-State Information Sharing and Analysis Center (MS-ISAC); the National Association of State Chief Information Officers (NASCIO); the National Coalition for the Prevention of Economic Crime (NCPEC); the National Electric Sector Cybersecurity Organization (NESCO); the National Security Institute; the National White Collar Crime Center; the System Administration, Audit, Network, Security (SANS) Institute; and US-CERT.

G. QUESTION 4: STATE DEFINITION OF NATIONAL CYBER INCIDENT

1. Findings

States C-4, E-5, M-13, O-15, P-16, and R-18 responded that they did not have a definition for a national significant cyber incident. The significant cyber incident term can be difficult to define: the basis of its significance may be subjective and based on the specific cyber mission space, e.g., finance, water, electricity, agriculture. A report conducted by the Center for Strategic and International Studies captured 84 significant cyber incidents from 2006 to 2011, based on a monetary threshold for distinguishing a significant cyber incident (Lewis, 2011). The report focused on successful attacks on government agencies and defense and high-tech companies or economic crimes with losses of more than one million dollars. This is a method that can delineate and provide thresholds for response to a significant cyber incident. Another method to identify a significant cyber incident could look at the threat perpetrator or the outcome of the

action, e.g., insider,,hacktivist, cyber criminal, individual hacker, accident, terrorist or denial of service, phishing, virus, trojan. Regardless of methodology, defining a significant cyber incident will provide a common element and understanding for response.

The NCIRP utilizes a risk-based approach that sets conditions in cyberspace; it requires increased national coordination for a significant cyber incident. This increase in national coordination is triggered when the NCRAL is set at “severe” or “critical.”

The NCRAL system takes into account the threats, vulnerabilities, and potential consequences across the cyber infrastructure. It is determined through the NCCIC and its partner organizations, which aggregate risk-based management activities to inform national-level risk and suggest appropriate national- and sector-level prevention and protection activities. State H-8 used the definition found in the NCIRP utilizing NCRAL risk indexing. Similarly States D-4, I-9, and Q-17 used a risk-indexing system. State I-9 used a color coded risk-indexing system. As mentioned above, DHS recognized challenges associated with color-coded alerting methodologies and replaced the HSAS with the non-color-coded NTAS.

State B-2 acknowledged the complexity of making such a determination, unless the event is a large-scale incident affecting interconnections with the federal government. Furthermore, State B-2 stated that improvements in information sharing between the various states and the federal government are required to determine such an occurrence; it is nearly impossible to do so on a day-by-day basis, considering daily threats, without improvements.

The National Response Framework identifies increasing conditions where a state’s capabilities will be insufficient or have been exceeded (DHS, 2008, p. 22). These conditions are requisite steps for a state to request federal assistance, including if appropriate, a Stafford Act presidential declaration of an emergency or major disaster. Like the NRF’s identification of increased conditions as a delineator, States F-6, G-7, J-10, K-11, L-12, and S-19 viewed a national significant cyber incident as an elevation of threats and vulnerabilities where larger geographic boundaries were involved and impacts

to critical infrastructure, national procedure, or economy would be part of the cyber incident. State K-11 used the explicit language that it would include large-scale cyber incidents that overwhelm the government and the private sector.

2. Key Patterns and Interpretations

Thresholds for a Course of Action: A threshold can give a recognized and documented change of state or boundary where different courses of action can be predefined. Establishing a fulcrum or tipping point where boundaries are crossed—such as large-scale incidents that affect interconnects with the federal government, larger geographic areas, impacts to critical infrastructure, or ones that overwhelm state and private-sector resources—could provide varying allocations and predefined desired outcomes.

H. QUESTION 5: KEY CONTACT FOR NATIONAL CYBER INCIDENT

1. Findings

States B-2 and K-11 said that, depending on the scale, an elevated senior official notification would happen that would include the governor and the governor's homeland security advisor respectively. As stated above, senior leaders should be made aware of the incident, but this should be done concurrently with those who can provide good information to the leaders, thus allowing a well-informed decision to be made by the senior leadership.

State D-4 stipulated that the key state individual who would be contacted for a national significant cyber incident would be the state's Infrastructure Protection Center, which is supported on a 24-hour basis. The state's Infrastructure Protection Center would coordinate the information with the state Network Operation Center and the statewide Information Security and Privacy Office. The approach of State D-4 appears to be comprehensive and provides information to many of the stakeholders involved. Similarly, State G-7 follows a systematic approach with the Department of Technology and Information, the chief security officer, the Department of Safety and Homeland Security,

the state Emergency Management Agency, and the state police high-tech crimes unit. It can be a fine line between informing the right stakeholders, those who can impact the outcome, and having to inform those who are just hungry for data. In a national significant cyber incident or any incident that has the potential for a broad information-hungry environment, this can be challenging task and one that needs to be managed as well. Moreover a 24-hour operational element used day to day, pre-incident, incident, post-incident, and back to day to day require different funding and management than one that is not. For a 24-hour operation, the staff size must accommodate a rotation of personnel, potential overtime hours, and possibly legal ramifications associated with federal, state, or union personnel laws.

Finally, States G-7 and R-18 included their departments of emergency management. Historically these departments are the incident management organizations that are at the forefront of any incident and traditionally approach the event using the ISC. The ISC has many years of being successfully utilized in physical geographic events. Cyber incident planning and responding can be a shift from traditional incident management like ICS. Cyber incidents could produce physical events, but their management most likely will happen virtually and independent of a geographic location. Moreover, the perpetrator of the event might be in another state or outside the borders of the United States.

2. Key Patterns and Interpretations

Regional Hubs: Utilizing a shared or common capability by region or at the national level for national significant cyber incidents could be a potential means to reduce resources and personnel cost. Collaborated plans, polices, and procedures would be required for a regional or national hub or node approach to allow effective and efficient information flow and action. A regional approach is not foreign to the federal government. The DHS Federal Emergency Management Agency is organized with 10 regional offices and the U.S. Customs and Border Protection of DHS has 20 regional field operations offices in the United States. As another example of a regional approach, the U.S. Army has chosen in its 2011 Posture Statement to include a regional approach,

called regional hub nodes. These focused force multiplier hubs provide satellite, voice, and data services to support forces as they flow into a theater of operations, including domestic disaster relief, and they enable deployed units to connect to Department of Defense networks.

I. QUESTION 6: KEY DEPARTMENT FOR NATIONAL CYBER INCIDENT

1. Findings

The answers to this question reveal a strong similarity to those organizations contacted for a state cyber incident discussed above in Question 3. States C-3, F-6, J-10, L-12, M-13, N-14, O-15, P-16, and R-18 all provided the same answer for this question and Question 3 above. This indicates that nine of the 19, or 47 percent, of the states from which the author received responses reported that the key department contacted does not change for a national significant cyber incident and a state cyber incident.

State B-2 elevated the notification to senior official organization as compared to those organizations contacted for State Cyber Incident. Similarly State G-7 elevated their contact organizations to senior levels and added the Chief Security Officer, Department of Safety and Homeland Security, State Emergency Management Agency and State Police High Tech Crimes Unit as compared to a State Cyber Incident. State K-11 added State Law Enforcement to the organizations like G-7.

Expanding the organizations for a National Significant Cyber Incident from a State Cyber Incident could introduce time drains as responders shift from one type incident to the other, so resource management should be considered.

2. Key Patterns and Interpretations

Unity of Effort: Having one organization for all cyber incidents could be of benefit with regard to timeliness of response and well-developed relationships and processes before a national cyber incident. Courses of action can require a cooperative approach involving numerous stakeholders. This can produce an effective and efficient

use of resources, but it requires mutual understanding of the capabilities, limitations, and consequences of actions. Unity of effort can also identify the ways in which capabilities best complement each other.

J. QUESTION 7: STATE CYBER INCIDENT ALERTING METHODOLOGIES

1. Findings

State B-2 addressed this question by identifying it use of formalized and published incident plans and an interagency state, federal, and private-industry incident response team as its alerting method procedure for cyber incident notification. With an official and published plan and procedure, a state can test and exercise the plan and implement lessons learned or alerting procedure refinements iteratively.

States C-3, F-6, G-7, H-8, J-10, and L-12 specified the use of e-mail as a method, but these states did not all rely exclusively on e-mail. State C-3 used text, phone, and an emergency notification system in addition to e-mail. State F-6 used the telephone and help desk escalation procedures. State G-7 also specified the telephone and added to e-mail subscription services and reverse 9-1-1.[5] State G-7's subscription service is available to the public and allows individuals access to various types of notifications. In addition to e-mail, State H-8 also includes two types of web-based portals: 1) an internal alerting tool that includes key state players, e.g., information security managers, the Department of Law Enforcement, the Division of Emergency Management, and enterprise information technology; and 2) the secure MS-ISAC portal. State J-10 also uses the MS-ISAC portal. State L-12 adds the telephone to its e-mail alert methods. Backup systems and methods give alternative avenues in the case of a system that becomes unavailable or disabled. Relying on telephone and e-mail alone could be a

[5] Reverse 9-1-1 is a commercially available public-safety communications system used by public-safety organizations and emergency managers to communicate with groups of people in a defined geographic area by sending prerecorded messages automatically by phone. The system uses a database of telephone numbers and associated addresses and can be tied into geographic information systems.

limiting factor to a cyber incident notification. Regardless of the number of backups, it can be important to test and exercise any process during down times or normal operation tempo as a preparatory position.

State D-4 described a systematic approach that includes plans, policy, and procedures. In State D-4, the state network operation center notifies the agencies' information security officers and privacy officers. In addition, the state infrastructure protection center communicates internal and external alerts. For compliance state agencies adhere to the statewide privacy policy. State D-4 addresses continuing compliance through an annual statewide policy and standards compliance assessment process that implements remediation or mitigation plans to correct gaps. Finally State D-4 uses its authority to disconnect noncompliant agencies from the statewide network.

State P-16 maintains a list of agency incident POCs that includes e-mail addresses, telephone, and cell phone numbers. For incidents with potential public exposure, State P-16 leverages the state communications office to manage press notifications; for incidents with law enforcement ramifications, the state works with the state police or leverages contacts in the FBI cyber crimes unit. Call lists or POC lists can be time consuming to maintain. During the research, some key state chief information officer positions underwent change; maintaining current contact lists could be problematic without the direct support of the departments and agencies responsible for the updates. Maintenance could be accomplished through a shared user name– and password-protected site where the updates could be made by each department, agency, or industry partner; this could alleviate the sometimes tedious task for one individual of tracking down the updated numbers.

State S-19 responded that for a catastrophic incident, in which the emergency operations center became engaged or activated, it would use WebEOC.[6]

[6] WebEOC is a commercially available product. It is a web-enabled crisis information management system that provides secure information sharing.

2. Key Patterns and Interpretations

Authorized and Published Plans, Policies, and Procedures: Authorized and published plans, policies, and procedures and their implementation enable the strategic or tactical transfer of intent, objectives, limitations, and desired outcomes for a cyber incident to the decision makers, givers of information, receivers of information, and those who take action on that information.

K. QUESTION 8: PREDOMINANT CAUSE OF STATE CYBER INCIDENT

1. Findings

States B-2, C-3, D-4, E-5, F-6, G-7, H-8, I-9, J-10, K-11, L-12, M-13, N-14, O-15, P-16, Q-17, and R-18, that is 17 of the 19 states, or 89 percent, stated that the predominant cause of a state cyber incident is cyber criminals. A 2011 cyber crime study independently conducted by Ponemon Institute and sponsored by ArcSight found that cyber attacks have become common occurrences and that the median annualized cost of cyber crime for 50 organizations in the study was $5.9 million per year. The companies in the study experienced 72 successful attacks per week and more than one successful attack per company per week (Ponemon Institute, 2011). It could be argued that numbers derived from companies that might have a vested interest in their resolution could be suspect, but the states' answers bring validity to the data, as does its independent study approach. Furthermore, regardless of how the numbers were derived, it is not uncommon to hear weekly national news outlets give headline stories about cyber criminal activities; to argue that this is not a substantial threat risks an unprepared position.

The next predominant cause identified was that of individual hacker. States D-4, F-6, G-7, H-8, I-9, J-10, K-11, N-14, P-16, and Q-17, that is 10 of the 19 states, or 53 percent, stated that this was a predominant cause of state cyber incidents. These hackers want to prove their skills and want to engage in unauthorized activities. This type of cause can be a nuisance, but it is important to recognize the threat in order to defend against it.

The next cause based on the numbers was that of insider. States E-5, F-6, G-7, I-9, J-10, O-15, and Q-17, that is 7 of the 19 states, or 37 percent, stated that this was a predominant cause of state cyber incidents. This cause could be an officemate motivated by revenge or greed.

Next in line was the hacktivist. States F-6, H-8, J-10, K-11, and Q-17, that is 5 of the 19 states, or 26 percent, stated that this was a predominant cause of state cyber incidents. The hacktivist could be motivated by political, religious, environmental, or other personal beliefs. His goal might be just to embarrass his opponents or deface their Web sites.

Two states saw "industrial and technology espionage and terrorism—exploiting" as a predominant cause of state cyber incidents. Of the 19 states that responded, other noteworthy but infrequent reponses included "terrorism." With the dynamic and open nature of cyberspace, it is naive not to consider all possibilities in planning.

Finally the category of "other" brought to light areas that should be considered. State D-4 commented that careless, nonmalicious, overworked, and unaware employees or vendors who did not follow processes, procedures, or quality assurance measures and out-of-date contract terms and conditions were causing approximately 70 percent of their potential incidents. State S-19 also pointed to human error or users unaware of the impact of their actions.

State P-16 brought up another key area that was not part of the causes presented in the questions: that of loss or theft of physical information security assets, such as laptops or paper.

Lastly, State N-14 observed that power outages and natural disasters are a cause of state cyber incidents. A power outage could either cause a state cyber incident, or it could be the outcome of a state cyber incident.

2. Key Patterns and Interpretations

Comprehensive and Adaptive Methods: Cybersecurity threats and vulnerabilities cover a large spectrum and can be adaptive; therefore, the methods to address them

require a comprehensive and adaptive approach. Unintentional human error, persistent actors who want to exploit the systems for intellectual, political, monetary, or personal gain, and nation states who want to do harm in the physical realm of power outages and natural disasters are all part of the cyberspace ecosystem and its security.

L. QUESTION 9: CURRENT RESPONSE TO STATE CYBER INCIDENT

1. Findings

States B-2, C-3, D-4, E-5, F-6, G-7, H-8, I-9, J-10, K-11, M-13, N-14, P-16, R-18, and S-19, that is 15 of the 19 states, or 79 percent, stated that they currently respond to a state cyber incident utilizing a state operation center. The responses of States C-3 and P-16 indicated that they do not have a state operation center but would use their state information system incident response team much like a center. State K-11 answered that it uses a formal ICS-type process that is activated—which they viewed as a state operation center. The types of state operation centers used were as follows: B-2 state security staff security operation center; D-4 state infrastructure protection center; E-5 information security operations center; F-6 department of information technology operations center; G-7 nothing specific; H-8 emergency operations center (EOC) and state network operation center; I-9 homeland security EOC; J-10 state security operation center; M-13 state operation center. State N-14 was not explicate but indicated that it has a designated and a backup site. State R-18 uses the state EOC or operates out of the information technologies agency; and S-19 uses the state EOC.

The following states indicated that they would use the state fusion center: D-4; F-6; G-7; H-8; J-10; K-11; O-15; and R-18. This equates to 8 of the 19 states, or 42 percent, who stated that they currently respond to a state cyber incident utilizing a state fusion center.

The principal information sharing and analysis center brought into play was the Multi-State (MS-ISAC). Every state that gave a response interacts with the MS-ISAC in some form. The various interactions included State B-2, with a comment that it was statically aligned with them; State C-3 saying that it would notify them; State F-6 adding

that this is how it would apply information sharing and collaboration with U.S. states and territories; and State I-9 stating that this is the organization upon which it depends the most and where it gets expert help. The Communication ISAC and the Information Technology ISAC were not given as entities utilized for response. Tapping and leveraging into defined and established capabilities can be an effective way to reduce costs and resource expenditures.

Lastly, although not completely absent, the DHS NCCIC and the DHS National Operation Center[7] (NOC) was not shown to be a go-to capability.

2. Key Patterns and Interpretations

Leverage Existing Capabilities: For a significant cyber incident the DHS NCCIC coordinates national response efforts. This 24/7 operational element of CS&C works directly with the federal, state, local, tribal, and territorial governments and private-sector cyber incident partners. The cyber ecosystem requires a coordinated and flexible system to detect threats and to communicate protective measures to the community it represents.

The state fusion center should be used to the fullest extent possible and could be used as capability force multiplier to share information and provide situational awareness to a larger community. State fusion centers can have information sharing technologies not always readily available to state centers and should be leveraged when feasible. The DHS NICC is a capability dedicated to protecting critical infrastructure essential to the nation's security, health and safety, and economic vitality, and it should be considered as well.

[7] The DHS NOC provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and in conjunction with the DHS Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

M. QUESTION 10: STATE RESPONSE TO NATIONAL CYBER INCIDENT

1. Findings

States C-3, D-4, E-5, F-6, G-7, H-8, I-9, J-10, K-11, M-13, N-14, P-16, R-18, and S-19, that is 14 of the 19 states, or 74 percent, stated that they currently respond to a national significant cyber incident utilizing a state operation center. The state operation centers were similar to those in Question 9 above but were was evaluated to more senior levels for a national significant cyber incident in only a few instances. The types of state operation centers used were as follows (those shown are only those with a different response from the one given for a state cyber incident): C-2 state EOC; D-4 state infrastructure protection center and the Department of Emergency Management and Military Agency EOC; G-7 Unified Command[8] at the state EOC. State S-19 discussed the use of the Catastrophic Cyber Disruption Plan (CDP) for communications and to guide response efforts in its response. The CDP provides emergency management and information technology entities in State S-19 with a communications, planning, and response framework to facilitate emergency management coordination within the state in the event of a catastrophic cyber-related disruption. The CDP is a subset of a regional plan that could expand or contract based on the magnitude of the effects.

The use of the state fusion centers was also similar to those answers provided for Question 9 above with the following notable exception: State F-6 would activate its cyber incident response plan, which will be discussed in the Chapter IV.

Finally States F-6, G-7, K-11, and O-15 all pointed out that for a national significant cyber incident, they would interact with the DHS NCCIC.

[8] Unified Command applies to the Incident Command System involving multiple jurisdictions or agencies. The Unified Command intent is to enable institutions and agencies with different legal, geographic, and functional responsibilities to coordinate, plan, and interact.

2. Key Patterns and Interpretations

Cyberspace Specific Planning: Explicit cyberspace planning, coordination, and execution among those who have a vested interest should include the full gamut of incident management that includes prevention, protection, response, and recovery. Using existing physical event plans without addressing any uniqueness associated with a geographic unencumbered virtual cyberspace event in that plan does not completely deal with all requirements. Utilizing existing plans as a starting point and allowing cyberspace nuances to be applied could render a solid position and a full gamut of incident management.

The research question posed was to establish a standardized operational cyberspace event, risk models, or alerting methodologies that could support states for a significant cyber incident, as defined by the NCIRP. Through the analysis and review of the answers provided by the states and the key patterns and interpretations above, methodologies that could support states for a significant cyber incident were analyzed, evaluated, and displayed. The key patterns and interpretations are summarized in their totality in below.

Table 2. Summary of Patterns and Interpretations of State Responses

• Key Patterns and Interpretations
• Use universally recognized and established definitions and terms for the federal, state, local, and industry cyberspace community.
• Employ a risk-based approach to cyber incident planning that gives a systematic and rigorous analysis methodology including remediation based on workflows and procedures.
• Leverage current or proven incident management systems, methodologies, or capabilities and alter if needed to adapt to the cyberspace mission space. • Help desk that allows the escalation of individuals or organizations being contacted • Statewide 24/7 incident hotline • Statewide 24/7 incident reporting • User name password-protected incident management Web portal • Ticketing reporting systems • Predefined and documented relationship with stakeholders • Predefined and automated notification and alerting system • MS-ISAC reporting process • Fusion centers • Open-source management tools • Online customer cyber incident reporting process • Web site with timestamp
• Understand, establish, and document the progression of responsibilities for cyber incident coordination and control
• Use cyber incident exercises to demonstrate competencies, strengths, and proficiencies and incorporate them to sustain and enhance existing capabilities
• Establish thresholds, fulcrums, or tipping points when predefined boundaries are crossed, instigating varying courses of action
• Understand a cooperative approach involving numerous stakeholders and the benefits of a unified cyber incident response effort
• Use comprehensive and adaptive cybersecurity methods that address the adaptive threat and vulnerability spectrum

• Use assessment, analysis, and authorities established to disconnect noncompliant agencies from statewide network.
• Authorize, develop, and document cyber incident–specific plans, policies, and procedures
• Consider predefined roles, responsibilities, privacy, and legal ramifications
• Institutionalize an annual statewide policy/standards compliance assessment process
• "Central Operation Center" communicates internal and external alerts to stakeholders
• Continued evaluation and review of existing alerts • US-CERT • MS-ISAC • Microsoft • IBM
• Assess, analyze, and use specialized incident response team
• Assess, analyze, and use regional cyber incident response and recovery relationships, including documented plans, policies, and procedures as appropriate
• Utilize federal grant process for cyber plans and procedures
• Maintain list of agency cyber incident federal, state, and local points of contact
• Legislate cyber policy and procedures
• Detail state cyber planners and subject matter experts to federal agencies and departments and detail federal cyber planners and subject matter experts to state agencies and departments

IV. RECOMMENDATIONS AND CONCLUSION

This research explored operational response constructs, risk models, and alerting methodologies that could support states for a significant cyber incident. The survey data collected from 19 states showed benefits in combining efforts that would be found in a regional approach and a need for cyber incident–specific planning. The regional approach allows the potential for sharing resources and knowledge. Specific planning that pertains to cyber incidents can give the response communities standard terms, definitions, and procedures. The literature reviewed showed the MOTR connected vested communities through teleconferencing. Through teleconferencing the MOTR collaborated situational awareness and actions. Recommendations will focus on cyber incident–specific planning, a regional hub construct, and the utilization of a federally facilitated significant cyber incident teleconference.

The need for improvement in information sharing between the various states and the federal government was revealed in the survey data. Specific cyber incident plans, a regional approach, and a facilitated significant cyber incident teleconference would support that. Furthermore, utilizing a shared or common 24/7 operation center and leveraging defined, funded, and established capabilities also revealed in the data would be addressed with specific cyber incident plans, a regional approach, and a facilitated significant cyber incident teleconference.

A regional-hub approach provides value for resource management, common plans, risk models, and notification alerting methods. The hub approach can provide shared funds execution and increased efficient and effective information flow and action due to the shared nature of the method. The hub could include boundary states, urban area security initiative sites, other key sites, and industry in those states. Regional hubs could facilitate hierarchal plans that could expand or contract based on the magnitude of the effects, where the local city plan would feed into the state plan and the state plan into the regional plan. The development, coordination, and execution of plans that focus on cyber incidents could benefit when done through a regional-hub construct as well.

The MOTR operational construct, configured for the cyber response community, could address improvements in information sharing between the various states and the federal government. The MOTR teleconference process utilizes a prearranged set of rules where federal officials coordinate their efforts to identify and mitigate risk. The MOTR notification process includes numerous agencies, designated experts, and command centers, as would be found in a regional approach. The MOTR provides a collaborative environment to develop courses of action in response to threats, as would be needed in a cyber incident. The MOTR process allows the contributing agencies to supply their subject matter expertise and capabilities to address the threat. Like the cyberspace domain, it requires a broad, collaborative approach to ensure that the desired outcome is fully discussed and fully informed by all the agencies with a stake in that outcome. A DHS-facilitated teleconference for a cyber incident could support a MOTR-like conference call among the state, industry, and the federal government.

The development of cyber incident plans has been augmented through the DHS grant program utilizing the Regional Catastrophic Preparedness Grant Program (RCPGP), which is administered by the FEMA grant programs directorate. When conditions were met, cyber activities have been funded under the DHS grant programs for state entities. It should be noted this method for cyber incident plan development requires that all documents and compliance conditions be met prior to any consideration.

The recommendation described above could be used as illustrated with the following: 1) cyber regional hubs established throughout the nation; 2) specific cyber incident hierarchal plans coordinated, developed, and executed that expand or contract based on the magnitude of the effects in the cyber regional hub construct; and 3) DHS CS&C-facilitated and maintained significant cyber incident teleconferencing for situational awareness, discussion, or courses of action with prearranged protocols where cyberspace federal, state, local, and industry stakeholders can coordinate their efforts to identify and mitigate risk in the cyberspace domain.

This research and its recommendations can provide the beginning components of a standard operating procedure (SOP) that would include the use of common terms and definitions, an acceptance of roles and responsibilities, regional constructs and their

interactions, teleconferencing procedures, training and exercise, and cyber plan development. For the purposes of this research, an SOP would be a written guideline that explains how an organization intends to operate and what is required of personnel in performing this operation for a given mission area, e.g., a cyberspace incident, and distills the important concepts, techniques, and requirements.

The SOP would need adaptive requirements and funding avenues developed with the cyber response community it would support. Those requirements would include the roles and responsibilities for the routine or day-to-day operations, as well as the high operational type. The responsibilities would discuss and determine the progression of coordination and control for the cyber incident. The requirements would also include the development of the cyber incident regional construct, which would review, leverage, and integrate valid existing procedures and protocols, organizations, and capabilities. With the regional construct defined, the cyber-specific planning would be documented, where thresholds for courses of actions, teleconferencing procedures, member requirements, training, and exercise would be ascertained.

The cyber-specific planning cannot just focus on the routine operations. It will require that the phases be defined when the need to elevate a cyber incident is evident. These would encompass the alert and notifications process and its trigger, response and recovery operations, and the deactivation as it progresses and swings back to routine operations. Finally an adaptable cyber incident approach must consider changes in the tactics of an adversary, the management of multiple cyber events, the security of the communications, expert, or surge capacity, and information management and its coordination.

This research revealed that the CISO is a key individual contacted for state cyber incidents, a requirement that state cyber incidents be reported, and the predominate cause of a state cyber incident as a cyber criminal. Furthermore, the research recognized that states use their authorities to disconnect noncompliant agencies from statewide networks. At the federal level, the discussions and implications of an “Internet kill switch” are

extremely contentious. Disconnecting noncompliant agencies from statewide networks is not a one-for-one equivalent to turning the public networks off, but it does have the same effect, that is, that the systems are disconnected from the users.

This research found that the use of personal contacts resulted in the most effective way to build the needed relationships and trust, which resulted in the questions answered. A response from a state that thought it was receiving questions of questionable intent would have been much different if the state knew who it was dealing with. The persistent research of finding an individual who knew me and then reaching out after that fact was the best means to finally make contact.

The findings of this cyber incident research led to the recommendations above through analysis of the approximately 227 answers from the questions developed, followed by telephone and in-person interviews. This process exposed the need for common terms and definitions, roles and responsibilities, standardized notification and reporting, adaptive methods, authorized and published plans, policies, and procedures, and the benefits of regional constructs.

This research does not exhaust the need for future research, due to the autonomy and unique relationships of the states with the federal government and the dynamic mission area of cybersecurity. Due to the limitation of time, some research was omitted. One area of future research is to conduct a comparative analysis of state cyber policy and standards as they relate to the overall security mission area that resides in cyberspace and that impacts an extremely diverse community of users with a wide range of needs. The significance of this research has applicability to the literature as it formulates and creates new data and information for the cyberspace ecosystem and its stakeholders, and it offers that same community and homeland security practitioners processes that could be replicated to respond and recover from a significant cyber event.

Cybersecurity is a serious challenge, and the Department of Homeland Security is continually making strides in improving the capabilities of the national homeland security enterprise and the manner in which cyberspace is represented in it. We must continue our efforts as a community of users to use our resources as efficiently and effectively as possible.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. NCIRP DEFINITION OF A SIGNIFICANT CYBER INCIDENT

A Severe or Critical incident on the Cyber Risk Alert Level System. A Significant Cyber Incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

A Significant Cyber Incident may destroy, degrade, or disrupt the cyber infrastructure and/or the integrity of the information that supports the private and public sectors. Complications from a Significant Cyber Incident may threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation. A Significant Cyber Incident may adversely affect the Nation's ability to project force and may have implications on the Nation's Strategic Deterrence capability. Rapid identification, information exchange, investigation, response, and remediation often can mitigate the damage that a Significant Cyber Incident can cause and aid in rapid recovery and reconstitution after and during an incident.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. STATE RESPONSES TO QUESTIONS

The following is the data received by all states for each of the survey questions. Due to the sensitivity of the data, the state is referenced only with an identifier key.

Table 3. Answers to Question 1

State Key	Question 1. How does your State define a State Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the state-level questions as defined from the policies at our state Web site.
B-2	Any activity whereby infection or unauthorized access occurs to the state's electronic information or telecommunication systems or facilities that house said systems or electronic information.
C-3	An incident that impacts a number of organizations, an incident that exposes sensitive information that can lead to identity theft or other types of theft.
D-4	See privacy policy and associated exhibits/standards below for details at our state Web site. P900 - Information Security Incident Management Policy E901 - Exhibit Data Classification Matrix E902 - Exhibit Executive Checklist E903 - Exhibit Glossary S905 - Incident Submission and Response Standard S910 - Data Breach Notification Standard
E-5	Our state characterizes information system security or cyber incidents as any event violating the state's security policy, standards, procedures, guidelines, processes or security best practice that may be detected as unexplained network or system behavior resulting in the loss of sensitive data or any instance where the state's reputation might suffer.
F-6	Any event(s) which breaches the confidentiality of data, or the unauthorized alteration of data, or the denial of availability of data/systems, unauthorized access, etc.
G-7	A violation or imminent threat against our state's assets. Source: Cyber Security Incident Response Team Policy.
H-8	A confirmed computer security event is a computer security incident. A computer security incident is any action or activity—accidental or deliberate—that compromises the confidentiality, integrity, or availability of the state's data and information technology resources.

I-9	Any adverse event that threatens the confidentiality, integrity or accessibility of an agency's information resources. These events include, but are not limited to, the following: Attempts (either failed or successful) to gain unauthorized access to a system or its data. Disruption or denial of service. Unauthorized use of a system for the transmission, processing or storage of data. Changes to system hardware, firmware or software without the agency's knowledge, instruction or consent. Attempts to cause failures in critical infrastructure services or loss of Critical Supervisory and Data Acquisition (SCADA) systems. Attempts to cause failures that may cause loss of life or significant impact on the health or economic security of the agency and/or State. Probing of any nature that an agency or other authorized entity has not approved in advance for system security testing purposes.
J-10	Security incidents include, but are not limited to events compromising or potentially compromising the security or integrity of the state's information technology resources.
K-11	In the state government space we consider a Cyber Incident to be one where data has been breached from one or more information technology resources; where a large number of resources have been infected or compromised or where a major application has been affected.
L-12	An adverse event originating from the Internet.
M-13	Any violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices that impacts one or more entities of the state and/or the state's network infrastructure.

N-14	We do not have a definition for a "state cyber incident." We have a definition for "incident" which is the NIST definition on page 89 of the document from this link: NIST Information Security Glossary of Key Information Security Terms http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. SOURCE: SP 800-61 Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: FIPS 200; SP 800-53 An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: CNSSI-4009
O-15	The Chief of the Office of Information Security shall investigate and resolve any breach of an information system of a state agency or elected officer that uses the equipment or services of the Department or an application of such an information system or unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system. From recent Legislature, waiting for Governor's signature (expected).
P-16	We don't define incidents as "Cyber" incidents—we define them as "Information Security" incidents. The distinction is that an information security incident can also involve paper or people, not just technology—"Cyber" incidents are a subset of Information Security incidents. By statewide policy, we define information security incidents as: "A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets, an agency, or third party and require non-routine preventative or corrective action." We further define a state information security incident as one that potentially impacts multiple state agencies or which pose a significant risk to the state. Because one of the major risks to the state includes the financial impact of Personal Identifiable Information (PII) breach and subsequent impact to state reputation, we prioritize incidents that result in an intentional or accidental PII breach.

Q-17	An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. This Information Technology Bulletin (ITB) establishes standard policies and processes for reporting and managing cyber security incidents. See #7 for Information Technology Bulletin (ITB) relating to State Cyber Incidents.
R-18	Any unauthorized access or potential unauthorized access to the state's electronic data.
S-19	A security incident is a suspected or real event that potentially threatens or damages state network resources, compromises the privacy, availability or integrity of confidential information, and impacts service delivery. Examples of security incidents include unauthorized probing, denial of service attacks, access to confidential and potentially identifying information, loss or theft of a device containing confidential information, alteration of data, and unauthorized modifications to network systems.

Table 4. Answers to Question 2

State Key	Question 2. Who is the key State individual that would be contacted for a State Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the State level questions as defined from the policies at our State web site.
B-2	The State Security Office would be contacted and depending on the scale either the state incident response commander or the Chief Security Officer (CSO).
C-3	State Chief Information Security Officer.
D-4	By statue/executive orders all agencies are to have a designated Information Security and Privacy Officers that are trained to communicate (via a secure web Management portal, hardcopy and/or phone) all potential incidents to the State Infrastructure Protection Center, for monitoring/management/escalation by the Statewide Information Security and Privacy Office.
E-5	State Chief Information Security Officer.
F-6	State Chief Information Officer and appropriate staff.
G-7	There is no single individual; our response process includes various stakeholders depending on the incident. All cyber incidents are coordinated through the Office of the Chief Security Officer.
H-8	State Chief Information Security Officer.
I-9	State Chief Information Security Officer.
J-10	Director of Access and Threat Assessment/Response.
K-11	Chief Information Security Officer.
L-12	State Chief Information Security Officer.
M-13	State Chief Information Security Officer.
N-14	We use an Information System Incident Response Team (ISIRT) that has an Incident Commander. This person could vary according to who is on-call. All incidents are recorded by the State Information Technology Services Division, Information System Security Officer.
O-15	State Chief of Office of Information Security.
P-16	We have a statewide Incident Hotline that is staffed by the state's Incident Response Team. The state's Incident Response Team is staffed under the State Chief Information Security Officer.

State Key	Question 2. Who is the key State individual that would be contacted for a State Cyber Incident?
Q-17	State Chief Information Security Officer, Deputy State Chief Information Security Officer, or Lead Incident Responder.
R-18	Legislation identifies the State Chief Information Officer who has designated the State Chief Information Security Officer to handle cyber security incidents.
S-19	State Chief Information Officer if statewide catastrophic potential; all other, primary Point of Contact is the Information Technology Security Group led by the Chief Information Security Officer.

Table 5. Answers to Question 3

State Key	Question 3. What Office/Department/Section does that key State individual work for that would be contacted for State Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the State level questions as defined from the policies at our State web site.
B-2	Department of Administration / Enterprise Technology Division / State Security Office.
C-3	State Security Office within the Department of Information Systems.
D-4	Department of Administration, Government Information Technology Agency, Statewide Information Security and Privacy Office (SISPO), State's CISO and Privacy Officer (PO).
E-5	Office of Information Security.
F-6	Bureau of Information Technology Services.
G-7	Department of Technology and Information.
H-8	Agency for Enterprise Information Technology. This Governor and Cabinet Agency houses the Office of Information Security which, by law is responsible for receiving all computer security incidents in State government.
I-9	Office of the CIO / Department of Administration / Enterprise Security Team.
J-10	Information Technology Division / Security Office / Access and Threat Assessment/Response Group
K-11	Department of Technology, Management and Budget / Office of Enterprise Security / Risk Management Section.
L-12	Office of Administration / Information Technology Services Division / Information Security Management Office.
M-13	State Information Security Division / Department of Information Technology Services.
N-14	Information System Security Office / State Information Technology Services Division / Department of Administration.
O-15	State Office of Information Security.
P-16	Office of the state CISO / Department of Administrative Services / Enterprise Security Office.
Q-17	State CISO, Deputy CISO, and the Lead Incident Responder.
R-18	The state Information Technologies Agency which is led by the state CIO. The CIO is appointed by the Governor and the CISO is hired by the CIO.
S-19	Department of Information Technology. If catastrophic event, the state Homeland Security and Emergency Management is engaged.

Table 6. Answers to Question 3A

State Key	Question 3A. How are reports gathered for a State Cyber Incident? *Note: States with "no response" to Question 3A provided answers prior to this new question being posed.*
A-1	No response.
B-2	No response.
C-3	Usually verbally with regular updates, also gather reports from technical resources to evaluate the malicious activity on the state network.
D-4	Via a secured Incident Management web portal that has multi-secondary feeds.
E-5	Our state utilizes an open customizable application that tracks incidents and identifies security issues.
F-6	Acquisition of logs from infrastructure components (firewalls, server, IPS, etc.), and coordination with the help desk for incident management.
G-7	No response.
H-8	No response.
I-9	No response.
J-10	Through tools and a ticketing reporting system.
K-11	No response.
L-12	On an ad hoc basis.
M-13	A security incident reporting guideline document and a security incident reporting form has been created and provided to our customers. Once an incident has been identified, our customers are to submit the report form, via email or fax. We are in the process of creating an online reporting application that our customers will be able to use to submit the incident information.
N-14	No response.
O-15	Currently a Computer Security Incident Response Team (CSIRT) form is used. In the near future web site with timestamp will be used.
P-16	Agencies are required by statute and policy to report agency information security incidents to the state Security Incident Response Team (SIRT). Those reports are made initially by telephone call but follow-up information gathering may be done by email or internal mail.
Q-17	Through a state online portal.
R-18	Calls can come to the state help desk, directly to the CISO/CIO, or through an online reporting form.
S-19	If potential incident the Information Technology Security Group (ITSG) point of contact, which logs the reported event, conducts the analysis, and coordinates necessary remediation/mitigation.

Table 7. Answers to Question 3B

State Key	Question 3B. Is there a requirement that State Cyber Incident be reported? *Note: States with "no response" to Question 3B provided answers prior to this new question being posed.*
A-1	No response.
B-2	No response.
C-3	Yes there is a requirement.
D-4	Requirements for reporting state incidents are found in state statute.
E-5	It is legislated and the state can take system offline.
F-6	Yes, through various federal regulatory and compliancy law and state statutes.
G-7	No response.
H-8	No response.
I-9	No response.
J-10	Yes there is a requirement.
K-11	No response.
L-12	If it meets certain requirements.
M-13	Yes there is a requirement.
N-14	No response.
O-15	Yes, through recent state statutes.
P-16	Yes, agencies are required by statute and policy to report information security incidents to the SIRT.
Q-17	Yes – Through this Internet portal.
R-18	The executive branch agencies are required to report within 24 hours of when they discovered or should have discovered the incident. The executive branch agencies do not include all of the higher education institutions.
S-19	Yes, via a security incident response policy and procedure.

Table 8. Answers to Question 3C

State Key	Question 3C. What level of involvement was your State engaged, with the coordination of the development of the DHS National Cyber Incident Response Plan (NCIRP)? *Note: Seven other states not recorded here were involved in NCIRP development meetings as shown in NCIRP partner collaboration documents.*
A-1	Yes. The State, through the MS-ISAC, participated with Cyber Storm III where the NCIRP was exercised. Additionally, our state participated in a statewide cyber security tabletop exercise sponsored by our Emergency Management Agency, which was produced under the advice of the DHS and FEMA. The purpose of the exercise was to provide participants with an opportunity to evaluate current concepts, plans, and capabilities for a response to a cyber attack against the state's computer networks and systems. The exercise was modeled after the Homeland Security Exercise and Evaluation Program (HSEEP). Multiple local, state, and government entities were involved in the exercise which included border state representatives.
B-2	No.
C-3	Did not respond to the question.
D-4	Did not respond to the question.
E-5	The State Chief Information Security Officer was not involved. *Note: Data shows they were involved as recorded in NCIRP development meeting documents with this State partner.*
F-6	Did not respond to the question.
G-7	Not involved directly but kept up to date on the progress through National Association of State Chief Information Officers and MS-ISAC.
H-8	We had minimal involvement and provided some comments. Would have liked to have been part of a workgroup.
I-9	State was given the opportunity to review for comments, but by the time it got to State CISO desk, it was too late for CISO to review it and provide the comments, so CISO just reviewed the draft. State Chief Technology Officer was asked by National Association of State Chief Information Officers to provide input and he passed it to CISO. CISO was to reply by e-mail.
J-10	Did not respond to the question.
K-11	Chief Information Security Officer was not personally involved but one of his colleagues was a reviewer.
L-12	Did not respond to the question.

State Key	Question 3C. What level of involvement was your State engaged, with the coordination of the development of the DHS National Cyber Incident Response Plan (NCIRP)? *Note: Seven other states not recorded here were involved in NCIRP development meetings as shown in NCIRP partner collaboration documents.*
M-13	No.
N-14	Input was provided through MS-ISAC.
O-15	Did not respond to the question.
P-16	No.
Q-17	Involved in the National Association of State Chief Information Officers Security and Privacy work group and provided feedback on the Plan draft through that forum.
R-18	Not sure with absolute certainty.
S-19	We had opportunity to provide input as a MS-ISAC active member.

Table 9. Answers to Question 4

State Key	Question 4. How does your State define a National Significant Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.
B-2	Our state has long since recognized the difficulties in making this determination, unless it is a large scale incident affecting interconnects with the federal government. Without significant improvements in the information sharing between the various states and federal government it is nearly impossible to make this determination on a day-by-day basis regarding our daily threats. Thus, our state partnered with the MS-ISAC and they feed all our threat traffic up to the federal SOC for evaluation.
C-3	I don't know that we would be the entity defining that term.
D-4	We do not categorize incidents as National, State or Local. Best practices dictate using High, Medium, Low risk rating scheme.
E-5	We don't have a definition for a National Significant Cyber Incident.
F-6	Any event which affects multiple states, regions or the entire country.
G-7	Incidents that impact critical infrastructure, national processes, and the national economy.
H-8	A Significant Cyber Incident is a set of conditions in the cyber domain that requires increased national coordination. This increase in national coordination is triggered when the National Cyber Risk Alert Level (NCRAL) system reaches Severe or Critical.

State Key	Question 4. How does your State define a National Significant Cyber Incident?
I-9	Though we may change it, we reference an older National Cyber Alert Indicator program definition: The following criteria set forth is the recommended agency actions and notification procedures for each alert level: A. Low (Green)—Indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses or other malicious activity. B. Guarded (Blue)—Indicates a general risk of increased hacking, virus or other malicious activity. The potential exists for malicious cyber activities, but no known critical exploits have been identified, or known exploits have been identified but no significant impact has occurred. C. Elevated (Yellow)—Indicates a significant risk due to increased hacking, virus or other malicious activity which compromises systems or diminishes service. Known vulnerabilities are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high. D. High (Orange)—Indicates a high risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high. E. Severe (Red)—Indicates a severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy, or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or wide spread level of damage or disruption of Critical Infrastructure Assets.
J-10	When it affects more than one state, or when MS-ISAC defines one.
K-11	Large-scale cyber incident that overwhelms government and the private sector. That requires national coordination.
L-12	An adverse, organized event originating from the Internet that targets local, state, federal, and private entities.
M-13	We do not have a specific definition for a national cyber incident. We would rely heavily on information that we receive from MS-ISAC for national cyber security events.
N-14	We do not have a definition for a state cyber incident. Our state uses the Department of Commerce, National Institute of Standards and Technology (NIST) definition for “incident” [United States Department of Commerce, 2011, p. 89].
O-15	No formal definition. Inferred by term.

State Key	Question 4. How does your State define a National Significant Cyber Incident?
P-16	We have no definition for a National Significant Cyber Incident. However, we work closely with MS-ISAC & DHS US-CERT and would follow-up with our contacts in our state if advised of a national incident.
Q-17	Security Incident Category 1 (Critical/High) The agency has determined that other organizations' systems are affected, such as business partners or outside organizations.
R-18	A formal definition has not been created to my knowledge. Anything that involves multiple states would likely trigger a national cyber incident.
S-19	Threats, attacks, disruptions, emergencies or disasters which impact national processes and economies including state and local government, private sectors and public.

Table 10. Answers to Question 5

State Key	Question 5. Who is the key State individual that would be contacted for a National Significant Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.
B-2	It would depend on the scale. Our governor, the Department of Military and Veteran Affairs, Homeland Security Division or the State Security Office all may be contacted depending on the incident, which individual discovered it, and the type of incident.
C-3	State Chief Information Security Officer.
D-4	The state's Infrastructure Protection Center that is supported 24/7, that immediately coordinates with the Network Operation Center / Security Operation Center function and the state's Department of Administration / SISPO State's CISO and PO.
E-5	State Chief Information Security Officer.
F-6	State CIO and appropriate staff.
G-7	Department of Technology and Information Chief Security Officer Department of Safety and Homeland Security State Emergency Management Agency State Police High Tech Crimes Unit
H-8	The Domestic Security coordinators in the Department of Law Enforcement and the Department of Management Services and the state CISO.
I-9	State CISO.
J-10	Director of Access and Threat Assessment/Response.
K-11	Governor's Homeland Security Advisor.
L-12	CISO.
M-13	The state Chief Information Security Officer.
N-14	We use an ISIRT that has an Incident Commander. This person could vary according to who is on call. All incidents are recorded by the state Information Technology Services Division, Information System Security Officer.
O-15	Chief of Office of Information Security.
P-16	We have a statewide Incident Hotline that is staffed by the State Incident Response Team (SIRT). The SIRT is staffed under the state Chief Information Security Officer.
Q-17	CISO, Deputy CISO and the Lead Incident Responder.
R-18	The CISO and/or the CIO. Depending upon the classification of "National Significant Cyber Incident" it may be the State Department of Emergency Management or the State Office of Preparedness.

State Key	Question 5. Who is the key State individual that would be contacted for a National Significant Cyber Incident?
S-19	The Homeland Security and Emergency Management (HSEM) Director who would engage the Department of Information Technology (DOIT) CIO.

Table 11. Answers to Question 6

State Key	Question 6. What Office/Department/Section does that key State individual work for that would be contacted for National Significant Cyber Incident?
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.
B-2	Governor's Office, Department of Military and Veteran Affairs, Homeland Security Division, or the Department of Administration, Enterprise Technology Division, State Security Office.
C-3	State Security Office within the State Department of Information Systems.
D-4	The state's Infrastructure Protection Center that is supported 24/7, that immediately coordinates with the Network Operation Center / Security Operation Center function and the state's Department of Administration / SISPO State's CISO and PO.
E-5	Did not respond to the question.
F-6	Bureau of Information Technology Services (BITS).
G-7	Department of Technology and Information Chief Security Officer Department of Safety and Homeland Security State Emergency Management Agency State Police High Tech Crimes Unit
H-8	State Department of Law Enforcement, Department of Management Services (DEM) and Agency for Enterprise Information Technology (AEIT).
I-9	Office of the CIO/Department of Administration/Enterprise Security Team.
J-10	Information Technology Division, Security Office, Access and Threat Assessment/Response Group.
K-11	State Police / Emergency Management Division.
L-12	Office of Administration, Information Technology Services Division, Information Security Management Office.
M-13	State Department of Information Technology Services / Information Security Division.
N-14	Department of Administration / State Information Technology Services Division / Information System Security Office.
O-15	Office of Information Security.
P-16	The Enterprise Security Office in the Department of Administrative Services (the CISO's office).
Q-17	Office of Administration (OA) / Office Information Technology (OIT) / Office for Information Security (OIS).

State Key	Question 6. What Office/Department/Section does that key State individual work for that would be contacted for National Significant Cyber Incident?
R-18	The CISO and CIO who work for state Information Technologies Agency.
S-19	Department of Safety, Homeland Security and Emergency Management.

Table 12. Answers to Question 7

State Key	Question 7. What alerting methodologies or procedures do your State use for a Cyber Incident notification?
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.
B-2	We have a formalized and published incident response plan, to include an incident response team that includes, state, federal and private industry specialist as members.
C-3	Email, text, phone, emergency notification system if warranted.
D-4	The Network Operation Center notifies agencies' Information Security Officer (ISO) and PO regarding specific potential low risks for mitigation based on workflows and procedures. State Infrastructure Protection Center (SIPC) communicates alerts (internal and external) to agency ISOs and POs for High/Medium risk remediation based on workflows and procedures. Agencies comply with statewide privacy policy. Annual statewide Policy/Standards Compliance Assessment process ensures that agencies/vendors are aware of, in compliance with and when required implementing remediation/mitigation plans to correct gaps. SISPO has authority to disconnect noncompliant agencies from statewide network.
E-5	Did not respond to the question.
F-6	E-mail, telephone, and help desk escalation procedures.
G-7	E-mail, subscription services, telephone, and Reverse 9-1-1.
H-8	SharePoint/Alerting tool to all the Information Security Managers in state government, state Department of Law Enforcement, DEM and AEIT. Secure MS-ISAC Portal E-mail.
I-9	Did not respond to the question.
J-10	E-mail and MS-ISAC portal.
K-11	We utilize the Multi-State ISAC reporting process.
L-12	Phone and e-mail.
M-13	We review alerts that we receive from various groups and organizations (MS-ISAC, Microsoft, IBM, DHS US-CERT, etc.). We provide the alerts to our customers via a statewide list and via our web page.
N-14	Our ISIRT uses phone, e-mail, an automatic alert system, and face-to-face communication, depending upon the event and any outage that is sustained.
O-15	Targeted notification to key ISOs, Fusion Center, and Infragard.

State Key	Question 7. What alerting methodologies or procedures do your State use for a Cyber Incident notification?
P-16	The SIRT maintains a list of agency Incident Points of Contact that we use to establish communications with agencies in the event of an incident. This includes e-mail addresses, telephone and cell phone numbers. We periodically send general-notification security alerts to our list of agency contacts (which includes some local government contacts). When working with agencies, we primarily work through their Points of Contact but will also jump to their ISO, CIO or director if necessary. For incidents with potential public exposure, we leverage our state communications office to manage press notifications. For incidents with law enforcement ramifications, we either work with the state police or leverage contacts in the FBI Cyber Crimes unit.
Q-17	We use the following state policies, procedures, forms, and standards. ITB-SEC024.doc - IT Security Incident Reporting Policy OPD-SEC024A - IT Security Incident Reporting Procedures OPD-SEC024B - IT Security Incident Reporting Form STD-SEC024C - Computer Incident Response Technology Standard
R-18	Security contacts exist at each agency as well as our Department of Emergency Management and the State Fusion Center. If the cyber incident is significant enough, all parties will be notified of the issue. If it is localized to specific agencies, they are notified.
S-19	For non-catastrophic, situational awareness notifications are provided for distribution. For catastrophic where the Emergency Operations Center (EOC) would become engaged and/or activated, WebEOC would be utilized.

Table 13. Answers to Question 8

State Key	Question 8. What is a predominant cause of a State Cyber Incident? • Insider. • Hacktivist. • Cyber Criminal. • Individual Hacker. • Industrial and Technology Espionage. • Terrorism—Connecting. • Terrorism—Cultivating. • Terrorism—Exploiting. • Other—Explain. *Note: "Cause" elaborations are included when provided by the state.*	
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.	
B-2	Cyber Criminal	This is by far the greatest number of incidents in the state, but this is closely related to Industrial and Technology Espionage. It is hard to make a determination of the motivation on many of our incidents.
	Industrial and Technology Espionage	The state believes this is closely related to the Cyber Criminals category and it is difficult to make a positive determination on many of our incidents.
C-3	Cyber Criminal	
D-4	Cyber Criminal	On-going and persistent threat.
	Individual Hacker	Mostly targeting vulnerable website for defacement purposes, or vendors trying to make a business case for providing risk vulnerability services.
	Other	Careless (non-malicious), overworked, unaware employees/vendors not following process/procedures or quality assurance measures.
E-5	Insider	
	Cyber Criminal	
F-6	Insider	
	Hacktivist	
	Cyber Criminal	
	Individual Hacker	
G-7	Insider	
	Cyber Criminal	

State Key	Question 8. What is a predominant cause of a State Cyber Incident? • Insider. • Hacktivist. • Cyber Criminal. • Individual Hacker. • Industrial and Technology Espionage. • Terrorism—Connecting. • Terrorism—Cultivating. • Terrorism—Exploiting. • Other—Explain. *Note: "Cause" elaborations are included when provided by the state.*	
	Individual Hacker	
H-8	Hacktivist	
	Cyber Criminal	
	Individual Hacker	
	Industrial and Technology Espionage	
I-9	Insider	Though this is a primary concern for me, we actually have not had any incidents identified in this category since I've been in this position.
	Cyber Criminal	This is by far the category that impacts us most often. Primarily web-based malware that is intended to steal information.
	Individual Hacker	This has happened, but rarely.
	Industrial and Technology Espionage	I prepared for this, but we've had no evidence that there have been any successful attacks in this category.
J-10	Insider	
	Hacktivist	
	Cyber Criminal	
	Individual Hacker	
K-11	Hacktivist	
	Cyber Criminal	
	Individual Hacker	
	Industrial and Technology Espionage	

State Key	Question 8. What is a predominant cause of a State Cyber Incident? • Insider. • Hacktivist. • Cyber Criminal. • Individual Hacker. • Industrial and Technology Espionage. • Terrorism—Connecting. • Terrorism—Cultivating. • Terrorism—Exploiting. • Other—Explain. *Note: "Cause" elaborations are included when provided by the state.*	
L-12	Cyber Criminal	
M-13	Cyber Criminal	The majority of the incidents involve malware and viruses.
N-14	Cyber Criminal	
	Individual Hacker	
	Other	Power outages, natural disasters, and/or accidents.
O-15	Insider	
	Cyber Criminal	
	Other	Nation State—Information Gathering. General Observation—Attribution is not always available. General Observation—List of causes is somewhat myopic.
P-16	Cyber Criminal	
	Individual Hacker	
	Other	Loss or theft of physical information security assets such as laptops or paper also constitutes information security incidents.
Q-17	Insider	
	Hacktivist	
	Cyber Criminal	
	Individual Hacker	
	Industrial and Technology Espionage	
	Terrorism—Connecting	
	Terrorism—Cultivating	

State Key	Question 8. What is a predominant cause of a State Cyber Incident? • Insider. • Hacktivist. • Cyber Criminal. • Individual Hacker. • Industrial and Technology Espionage. • Terrorism—Connecting. • Terrorism—Cultivating. • Terrorism—Exploiting. • Other—Explain. *Note: "Cause" elaborations are included when provided by the state.*	
	Terrorism—Exploiting	
R-18	Cyber Criminal	Recently we primarily see malware exploits and attempts to steal credentials and money.
	Other	We have had all types of cyber incidents throughout the years. While they now focus on malware to steal money and credentials, we have had hacktivist, insider threats, and individual hackers. Determining motives can also be difficult so it is possible espionage may have been involved.
S-19	Other	Human error or users unaware of the impact of their actions.

Table 14. Answers to Question 9

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
A-1	Please review the links and gather the appropriate responses to the State level questions as defined from the policies at our State web site.	
B-2	State operation center	The State Security Staff runs a security operation center internal to the state during normal business hours but we heavily rely on the MS-ISAC for our day-to-day security threat detection and initial analysis.
	Homeland Security Advisor	The state has a strong relationship with our Protective Security Advisor and routinely keeps them informed regarding our situational awareness for cyber threats and incidents.
	MS-ISAC	Our State is one of the founding members on the MS-ISAC services. We are strategically aligned with the MS-ISAC on all our threat monitoring and security services.
	Other	The State has a strong partnership with the FBI and we provide information and awareness of all our threats to them.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
C-3	State operation center	A team is activated in the event of a significant cyber event made up of individuals of the Department of Information Systems.
	Homeland Security Advisor	We would notify the director of the Department of Emergency Management.
	MS-ISAC	We would notify the MS-ISAC through their portal or by phone.
	Other	InfraGard[9] Members Alliance would be notified if the threat was relevant to the members.
D-4	State operation center	The function—State Infrastructure Protection Center (SIPC) and the office—Statewide Information Security and Privacy Office (SISPO).
	State Fusion Center	Primarily a law enforcement (sworn officer) function that focuses on Critical Infrastructure Protection for the private sector.

[9] InfraGard is an information sharing and analysis effort that serves the interests and combines the knowledge base of a wide range of members. InfraGard is a partnership between the Federal Bureau of Investigation and the private sector, but it also includes an association of businesses, academic institutions, state and local law enforcement agencies, and other participants.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	Homeland Security Advisor	Not a priority—all funding for Incident Management is the state's.
	MS-ISAC	MS-ISAC provides Point of Contact support for interacting with DHS, DHS US-CERT, and FBI.
	Other ISAC	Utilize State Network Operation Center to prevent, monitor, and remediate at perimeter. State CIO Council, ISO / PO Community of Interest Governance body, with statute/policy monitoring/compliance enforcement to ensure that business practices and control are in place. The SIPC function manages incident documentation, workflow, and communications. The SISPO oversees entire Incident Management activity statewide.
	Other	Support FBI cyber function. Also work with state's Department of Emergency Management and Military Agency (DEMA) to support Statewide Emergency Response and Response Plan (SERRP) Cyber Annex and Continuity Operations Program's IT Disaster Recovery Planning.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
E-5	State operation center	State Information Security Operations Center (ISOC).
	MS-ISAC	Only for incidents that would change our state MS-ISAC Cyber Alert indicator. By changing our Cyber Alert indicator, MS-ISAC would coordinate information gathering and sharing processes with us and other states.
	Other	In some cases, we would contact the state's Bureau of Investigations or the FBI.
F-6	State operation center	Utilize the state's DOIT operations center. The operations center is manned with state staff computer operators with specific escalation procedures and staff to contact.
	State Fusion Center	There is a separate fusion center which can be utilized in a significant national event.
	Homeland Security Advisor	The Homeland Security Advisor is utilized when working with the MS-ISAC and the DHS US-CERT during incident response activities.
	MS-ISAC	Information sharing and collaboration with U.S. states and territories. Emergency response in significant national events.
	DHS NCCIC	Through the state Fusion Center.
	DHS National Operation Center	Through access and collaboration with the DHS US-CERT.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
G-7	State operation center	State has an operation center that would be used.
	State Fusion Center	The state Fusion Center would be part of the incident response team.
	Homeland Security Advisor	The state HSA would be part of the incident response team.
	MS-ISAC	We would rely on their alerts and request assistance as needed.
H-8	State operation center	Emergency Operations Center, MS-ISAC Cyber Security Operations Center, state's Network Operation Center, NCCIC and DHS US-CERT would all be working together.
	State Fusion Center	State CISO is a member of the Domestic Security Task Force, Law Enforcement Terrorism Prevention Committee, Domestic Security Oversight Council and Fusion Center.
	Homeland Security Advisor	The HSA would be utilized, but they are not very engaged in cyber issues.
	MS-ISAC	See other answers.
	DHS NCCIC	See other answers.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
I-9	State operation center	In theory, the Bureau of Homeland Security Emergency Operation Center would be used. Planning to exercise this is being conducted.
	Homeland Security Advisor	We have been in contact with our HSA, but it is sporadic.
	MS-ISAC	By far, this is the organization that we depend on the most. We send meaningful information to them and they provide expert help, if needed, and advice that is always useful.
J-10	State operation center	We coordinate through the state's Security Operation Center in one of our major cities. All coordination, correlation and tracking of events.
	State Fusion Center	Information sharing is conducted.
	MS-ISAC	All incidents during an event (not a single incident) are reported and coordinated through the MS-ISAC.
K-11	State operation center	Our department has a formal Incident Command System type process that gets activated during an incident.
	State Fusion Center	We send cyber-related information to the Fusion Center for their situation awareness.
	MS-ISAC	They are notified of major incidents.
	DHS NCCIC	Through the MS-ISAC.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	DHS National Operation Center	Through the MS-ISAC.
	DHS NICC *only small instances of this*	Through the MS-ISAC.
L-12	MS-ISAC	Leverage communication channels that MS-ISAC provides.
M-13	State operation center	Our Operation Center would be used primarily for customer updates and information distribution.
	MS-ISAC	Our state has a strong relationship with the MS-ISAC and would keep them involved throughout the entire process.
N-14	State operation center	We have a formal plan with a designated site and backup site.
	MS-ISAC	Used for research and information purposes.
O-15	State Fusion Center	They would be notified.
	Homeland Security Advisor	Would be used as a pass through to Federal Officials.
	MS-ISAC	Utilized through notification, analysis, and coordination.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	Other	DHS US-CERT analysis would be utilized. Communicate with key private sector individuals with whom I have a relationship for correlation of information.
P-16	State operation center	The SIRT, although not an operations center, leads and coordinates multi-agency incident response activities. The SIRT also performs technical and forensic analysis for agencies.
	MS-ISAC	Provide incident information and coordinate for multi-state incident exercises. In the event of activity we detect with potential multi-state impact we would leverage MS-ISAC for communications and contacts.
	Other	Depending upon the nature and scope of an incident, the SIRT may rely upon agency incident response personnel and/or technical personnel at our consolidated State Data Center. Also, depending upon the scope and nature of the incident, we may involve our partners in law enforcement or the FBI.
Q-17	MS-ISAC	We utilize the MS-ISAC capabilities.
R-18	State operation center	Depending upon the situation there is an emergency operations center or it could operate out of state Information Technologies Agency.

State Key	Question 9. How does your State currently respond to a State Cyber Incident? • State has an operation center that would be used for a State cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	State Fusion Center	State Information Technologies Agency coordinates with the Fusion Center on any significant cyber issues.
	Homeland Security Advisor	This happens through the Fusion Center or the state's Office of Preparedness.
	MS-ISAC	Any significant issues will be communicated out to the community. There have not been any significant outbreaks to cause us to utilize them.
S-19	State operation center	If catastrophic event, the state Emergency Operation Center would be engaged and/or activated.
	MS-ISAC	If catastrophic event, the State Emergency Operation Center would be engaged and/or activated.
	Other	For routine reported events, the IT Security Group logs and investigates internally.

Table 15. Answers to Question 10

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
A-1	Please review the links and gather the appropriate responses to the state level questions as defined from the policies at our state web site.	
B-2	No comment.	
C-3	State operation center	We would activate our team in conjunction with the state's Department of Emergency Management. We would respond to the event from the state emergency operations center.
	MS-ISAC	We would communicate with the MS-ISAC via the portal and by phone.
	Other	We would participate with the state InfraGard chapter by e-mail.
D-4	State operation center	The state Network Operation Center, with agencies, SIPC, and SISPO would support/facilitate internal remediation, while the DEMA Emergency Operation Center would manage/coordinate external recovery and remediation efforts.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	MS-ISAC	Use the MS-ISAC to share cyber remediation information between states and coordinate with DHS and DHS US-CERT.
E-5	State operation center	State Information Security Operations Center.
	MS-ISAC	Coordinated information from the MS-ISAC on incident.
F-6	State operation center	The Department of Information Technology Operations center would be used for coordinating response in a National cyber event.
	State Fusion Center	Activation of Cyber Incident response capability.
	Homeland Security Advisor	In a National cyber event, the DHS Security Advisor would be contacted.
	MS-ISAC	Communication with the MS-ISAC members, utilization of the fusion center there, coordination with other states' fusion and operation centers.
	DHS NCCIC	In a national cyber event, the NCCIC will be contacted and included and state efforts.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	DHS National Operation Center	In a national cyber event, the DHS US-CERT at the DHS National Operation Center would be contacted and included and state efforts.
	DHS NICC	In a national cyber event, the NICC will be contacted and included and State efforts.
	Other	State's Private Sector Working group is utilized.
G-7	State operation center	Unified Command would be established at state's Emergency Management Agency.
	State Fusion Center	State Fusion/State Police would be a member of unified command.
	Homeland Security Advisor	HAS would be member of Unified Command.
	MS-ISAC	MS-ISAC would be member of Unified Command.
	DHS NCCIC	As required, coordinated by MS-ISAC most likely.
H-8	State operation center	Emergency Operations Center, MS-ISAC Cyber Security Operations Center, state's Network Operation Center, NCCIC and DHS US-CERT would all be working together.
	State Fusion Center	State CISO is a member of the Domestic Security Task Force, Law Enforcement Terrorism Prevention Committee, Domestic Security Oversight Council and Fusion Center.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	Homeland Security Advisor	The HSA would be utilized, but they are not very engaged in cyber issues.
	MS-ISAC	See other answers.
	DHS NCCIC	See other answers.
I-9	State operation center	In theory, the Bureau of Homeland Security Emergency Operation Center would be used. Planning to exercise this is being conducted.
	Homeland Security Advisor	We have been in contact with our HSA, but it is sporadic.
	MS-ISAC	By far, this is the organization that we depend on the most. We send meaningful information to them and they provide expert help, if needed, and advice that is always useful.
J-10	State operation center	We coordinate through the state's Security Operation Center in one of our major cities. All coordination, correlation, and tracking of events.
	State Fusion Center	Information sharing is conducted.
	MS-ISAC	All incidents during an event (not a single incident) are reported and coordinate through the MS-ISAC.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
K-11	State operation center	State Security Operation Center (SEOC) would be activated.
	State Fusion Center	Information is exchanged between State Fusion, SEOC, and the state's Security Operations group.
	Homeland Security Advisor	The governor's Homeland Security Advisor is Director of State Police. That directs emergency management.
	MS-ISAC	Information is regularly passed between MS-ISAC and the States in the form of alerts and conference calls.
	DHS NCCIC	Information comes via the MS-ISAC.
	DHS National Operation Center	Information comes via the MS-ISAC.
	DHS NICC	Information comes via the MS-ISAC.
L-12	MS-ISAC	Leverage communication channels that MS-ISAC provides.
M-13	State operation center	Our Operation Center would be used primarily for customer updates and information distribution.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	MS-ISAC	We would stay in close contact with the MS-ISAC to make sure that we have the latest information.
N-14	State operation center	We have a formal plan with a designated site and backup site.
	MS-ISAC	Used for research, intelligence, and information purposes.
O-15	State Fusion Center	Communication and notification.
	Homeland Security Advisor	As a pass through to federal officials.
	MS-ISAC	Notification, analysis, and coordination.
	DHS NCCIC	Notification, analysis, and coordination.
P-16	State operation center	The SIRT, although not an operations center, leads and coordinates multi-agency incident response activities. The SIRT also performs technical and forensic analysis for agencies.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
	MS-ISAC	We use the MS-ISAC provided incident information and work with them for multi-state incidents, if one were to come up. In the event of activity we detect with potential multi-state impact, we would leverage MS-ISAC for communications and contacts.
	Other	We have worked with the FBI on multi-state criminal computer information security incidents. We would also rely on our agency and state data center personnel to assist with response to a National Significant Cyber incident.
Q-17	MS-ISAC	We utilize the MS-ISAC capabilities.
R-18	State operation center	Depending upon the situation there is an emergency operations center or it could operate out of state Information Technologies Agency.
	State Fusion Center	State Information Technologies Agency coordinates with the Fusion Center on any significant cyber issues.
	Homeland Security Advisor	This happens through the Fusion Center or the state's Office of Preparedness.
	MS-ISAC	Any significant issues will be communicated out to the community. There have not been any significant outbreaks to cause us to utilize them.

State Key	Question 10. How would your State respond to a National Significant Cyber Incident? • State has an operation center that would be used for a National cyber event? • State Fusion Center utilized? • Homeland Security Advisor utilized? • Multi-State Information Sharing and Analysis Center (MS-ISAC) utilized? • Communications ISAC utilized? • Information Technology ISAC utilized? • Other ISAC utilized? • DHS National Cybersecurity and Communications Integration Center (NCCIC) utilized? • DHS National Operation Center (NOC) utilized? • DHS National Infrastructure Coordinating Center (NICC) utilized? • Other—Explain.	
S-19	State operation center	Catastrophic CDP would be utilized for communications and to guide response efforts.
	MS-ISAC	Event would be reported to MS-ISAC and advice solicited. Contact with other impacted states would be initiated.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. NATIONAL CYBER INCIDENT RESPONSE PLAN QUICK REFERENCE GUIDE

Significant Cyber Incident: A Significant Cyber Incident is a set of conditions in the cyberspace that requires increased national coordination. This increase in national coordination is triggered when the National Cyber Risk Alert Level (NCRAL) is set at Severe or Critical.

The NCRAL system takes into account the threats, vulnerabilities, and potential consequences across the cyber infrastructure and provides an indication of the overall national cyber risk.

Normal	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities or activities—pose no significant risk to CIKR sector core critical functions or operations.[10]
Guarded	Vulnerability and cyber incident reporting and analysis indicate that information and communication technology may be disrupted or degraded or at greater risk of disruption or degradation, however, impact on core critical functions across the CIKR sectors is manageable by the responsible owners and operators. Standard, "steady state" protective measures, procedures, and monitoring are generally adequate to protect systems. However, enhanced security measures may be required.
Elevated	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities or activities place core critical functions across the CIKR sectors at serious risk of being degraded or disrupted. Preparedness, mitigation, or response measures are able to be maintained indefinitely as a part of normal operations.

[10] While core critical functions will differ across industries and sectors, an example of critical functions for the IT sector are outlined in the IT Sector Risk Assessment. These critical functions support the IT sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. These critical functions include: Produce and Provide IT Products and Services; Provide Domain Name Resolution Services; Provide Internet-based Content, Information, and Communications Services; Provide Internet Routing, Access and Connection Services; and Provide Incident Management Capabilities.

Severe	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities are compromising, degrading and/or destroying core critical functions across or within one or more CIKR sectors. Preparedness, mitigation, or response measures are only possible at a significant and indefinitely surged posture.
Critical	Current cyber threat actor behavior, system/hardware vulnerabilities and activities have resulted in the total or near total compromise and disruption across multiple CIKR sectors. Mission-critical cyber systems have been seriously and widely degraded, or destroyed threatening the homeland security, national security or continued operation of government or CIKR functions. No known mitigation methods or existing response actions are overwhelmed.

During a Significant Cyber Incident, DHS, through its National Cybersecurity and Communications Integration Center (NCCIC), coordinates national response efforts and works directly with Federal, State, local, tribal, and territorial governments and private sector partners.

APPENDIX D. NATIONAL CYBER RISK ALERT LEVEL SYSTEM SUMMARY

The National Cyber Risk Alert Level (NCRAL) system is the United States's national alert mechanism focused on risk in cyberspace, including risk to other CIKR sectors originating from cyberspace. It is a tool for maintaining public and private sector awareness of and stimulating preventative, consequence management or response actions to, known and potential threats to:

- Information and communications technology infrastructure,
- Critical information that transits or resides on that infrastructure, and
- Risks to critical infrastructures or key resources that may be disrupted via cyberspace.

As an alerting mechanism among public and private sector partners, the NCRAL contributes to shared situational awareness, supports decision making, encourages information sharing, and informs cyber incident management activities. During a Significant Cyber Incident, or in anticipation of one, the NCRAL serves as a catalyst and driver for nationally-coordinated response actions, specifically across the U.S. Government.

The NCRAL system leverages the shared situational awareness developed by the National Cybersecurity and Communications Integration Center (NCCIC) to inform the NCRAL alert level. There are five risk alert levels of increasing severity:

Normal	Guarded	Elevated	Severe	Critical

Cyber Risk

The NCRAL system enables an evaluation of risk to the information and communication technologies[11] that support the Nation's security, public health and safety, economic vitality, and way of life. It examines the following risk factors:

[11] The NCRAL also considers the risk to information that is stored and transmitted via information and communications technologies.

- Threats: Activities, actors, and event indicators of a potential cyber incident.
- Vulnerabilities: Physical or logical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.
- Consequences: Effect of an event, incident, or occurrence, including abnormal performance or degradation of critical national functions.

Determining National Cyber Risk

The NCCIC and its partner organizations conduct risk management activities, which are aggregated by the NCCIC to inform national-level risk and suggest appropriate national and sector-level prevention and protection activities. The NCCIC also conducts continual analysis of private and public sector risk/alert levels and the information that contributes to setting those alert levels. [12] This in turn allows DHS to examine changes in other alert levels to assess and communicate national-level risk.

To determine national cyber risk, both cyber and non-cyber activities are analyzed to determine overall risk of disruption, degradation or physical damage to IT and communications infrastructure and the Nation's other CIKR sectors. This includes incorporating sector-specific risk assessment models and frameworks, and identifying intersections among them.

The NCCIC determines cybersecurity risk and establishes proactive protective measures by:

- Conducting a comprehensive, on-going, and collaborative assessment of the national cyber common operational picture. This occurs in consultation with critical partners using information from all sources and taking into account threat, vulnerability and consequence information.
- Maintaining awareness of other risk/alert systems within the federal, defense, and state and local communities and critical infrastructure sectors.
- Conducting analysis of the capabilities that affected communities and organizations have to effectively counteract threats and mitigate vulnerabilities or consequences.
- Validating technical analysis and evaluation of relevant threat, vulnerability, and incident information and impact to information and communication technology.

[12] Examples of some of these risk/alert systems and protocols are the NCRAL, CYBERCON, INFOCON, and Information Sharing and Analysis Centers (ISAC) alert levels such as the Multi-State ISAC, Information Technology ISAC and Financial Sector ISAC.

- Estimating the possibility for the rapid escalation of a threat and/or exploitation of a vulnerability, and the potential impact of the escalated risk to critical mission and/or business operations.
- Determining potential national-level consequences affecting Nation's security, public health and safety, economic vitality, and way of life.
- Assessing likely effectiveness of available mitigation capabilities to prevent or diminish the impact of risk.

These factors provide the basis for determining the current level of cyber risk to national-level critical functions. Figure 1 is an overview of the assessment methodology that is used to determine the NCRAL and Table 1 provides a high-level overview of the NCRAL.

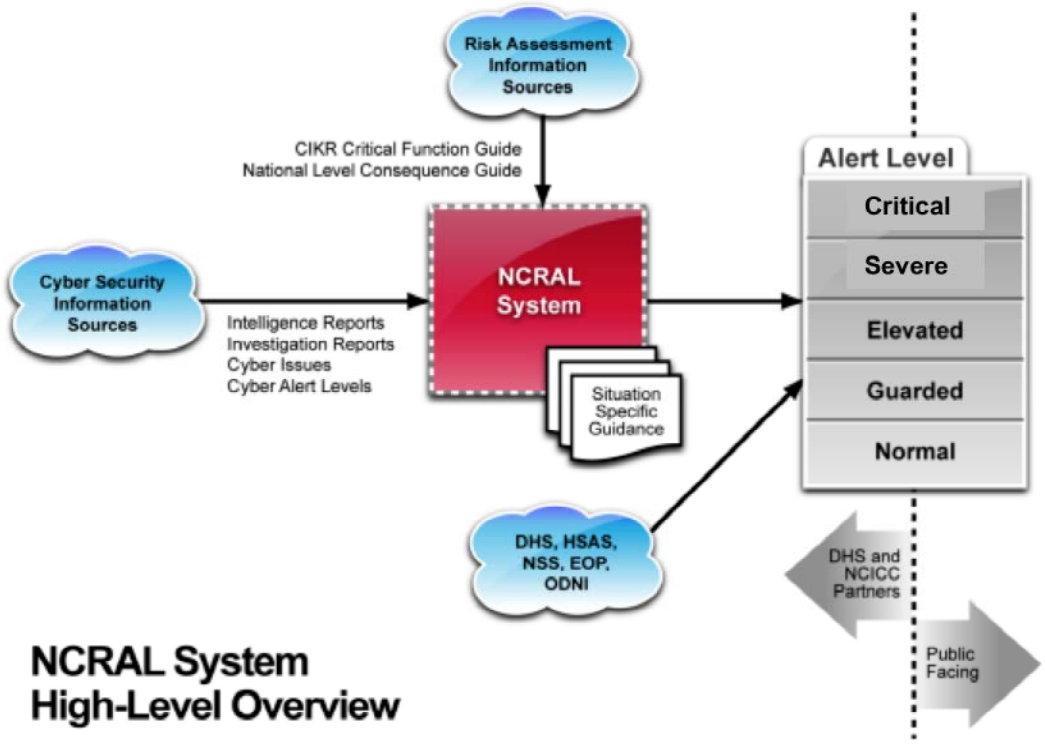

Figure 1. NCRAL System High-Level Overview (from DHS-CS&C, 2011)

Setting the Alert Level

The threat, vulnerability and consequence data related to the impact to CIKR are analyzed to determine:

- Probability of the impact (Is this a potential or suspected impact? Are there observed indications that the impact is occurring or about to occur?)
- Extent and severity of the potential/observed impact (Is the potential/observed impact minimal, moderate, significant or severe?).[13]

This is done by:

- Identifying the type of threat (e.g., zero-day, malicious code, distributed denial of service attack).
- Determining the characteristics or parameters of the threat (e.g., successful or unsuccessful, widespread or localized, release date known / unknown, indications or confirmed intelligence reporting.
- Identifying and analyzing the vulnerable information and communication technology (e.g., mission critical, non-mission critical).
- Determining the impacted CIKR sector(s) and critical functions.

The assessment will be aggregated by the NCCIC in collaboration with its other CIKR partners and evaluated against the impact descriptions provided in Table 1 to determine the overall alert level. Each level describes general, but not all-inclusive conditions that may exist at each alert level, and identifies broad guidelines for reporting, mitigation, analysis, and other actions.

[13] Minimal: activity results in minimal disruption, normal operations is sufficient for response management; Moderate: activity results in technology not being substantially degraded, normal operations or temporary surge operations required for response management; Significant: activity causes degradation technology and normal operations overwhelmed and surge response is indefinitely necessary; Severe: activity is or projected to be highly disruptive, response operations are overwhelmed.

Table 16. National Cyber Risk Alert Levels

Label	Description	Expected NCCIC Actions	Suggested Community Actions
Normal	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities or activities pose no significant risk to CIKR sector(s) core critical functions[14]	• The NCCIC, partners and constituents maintain routine coordination activities and other operational relationships in order to maintain a common operating picture to assess cyber risk	• Ensure policies, procedures and processes that support normal baseline operations conforms with best practices provided through nationally and internationally recognized organizations, such as the National Institute of Standards and Technology - Continuous identification and monitoring of critical systems that support organization / sector critical functions • Maintain system monitoring and conduct timely update with indicators and signatures - Continue to patch systems regularly and monitor all systems for known threats and anomalous activity

[14] While core critical functions will differ across industries and sectors, an example of critical functions for the IT sector are outlined in the IT Sector Risk Assessment. These critical functions support the IT Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. These critical functions include: Produce and Provide IT Products and Services; Provide Domain Name Resolution Services; Provide Internet-based Content, Information, and Communications Services; Provide Internet Routing, Access and Connection Services; and Provide Incident Management Capabilities.

Label	Description	Expected NCCIC Actions	Suggested Community Actions
Guarded	Vulnerability and cyber incident reporting and analysis indicate that information and communication technology may be disrupted or degraded or at greater risk of disruption or degradation, however, impact on core critical functions across the CIKR sectors is manageable by the responsible owners and operators. Non-cyber reporting indicates that conditions may exist for escalating risks these core functions: • Current known vulnerability or threat activity poses an identifiably higher risk of disruption or degradation to systems that support critical functions to the organization / sector • Current attacks conform to mostly known methods and sources Standard, "steady state" protective measures, procedures, and monitoring are generally adequate to protect systems However, enhanced security measures may be required.	• NCCIC maintains steady-state operational tempo to include routine coordination calls with partners and reporting • NCCIC and members of the Cyber UCG may increase focused planning in preparation for the potential of rapid risk escalation	• Continue to conduct suggested community activities outlined for Normal. • Ensure the organization is prepared to respond to an incident that poses a greater risk to the organization • Conduct appropriate information sharing relationships to support cyber response activities - Continually assess vulnerability and mitigating actions for systems that support organization / sector critical functions

Label	Description	Expected NCCIC Actions	Suggested Community Actions
Elevated	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities or activities place core critical functions across the CIKR sectors at serious risk of being degraded or disrupted. - Evidence exists of successful attacks that affects systems critical to CIKR critical functions, to include command, control and communication systems, but does not substantially degrade them • Strategies to mitigate the successful attack are available and distributed • Preparedness, mitigation, or response measures are able to be maintained indefinitely as a part of normal operations	• NCCIC increases its operational tempo to include frequent scheduled coordination calls with partners and reporting on a more frequent basis, as required by the incident • Increased operational tempo of the Cyber UCG Staff, discuss notification of Cyber UCG Senior Officials • NCCIC Planning Group and partners participate in interagency planning efforts • Direct outreach and coordination with targeted/affected entities, and with those who may be targeted or affected • Evaluate assistance that may be required, especially as related to HSPD-5.	• Continue to conduct suggested community activities outlined for Guarded. • Implement mitigation strategies, as disseminated within the Sector and from DHS, to reduce the risk of the threat / vulnerability to include increased level of monitoring to assess risk of exposure. - Provide event-specific communications, through the appropriate reporting channels (e.g. ISACs, Cyber Centers) to support the NCCIC's situational awareness and assessment of the threat.

Label	Description	Expected NCCIC Actions	Suggested Community Actions
Severe	Current or predicted cyber threat actor behavior, system/hardware vulnerabilities are compromising, degrading and/or destroying core critical functions across or within one or more CIKR sectors: • Major disruption to critical functions is imminent or in progress as impacts to mission critical systems are occurring • An attack on systems critical to CIKR critical functions, to include command, control and communication systems of national significance is occurring. Preparedness, mitigation, or response measures are only possible at a significant and indefinitely surged posture	• NCCIC increases its operational tempo to include frequent scheduled coordination calls with partners and reporting on a more frequent basis, as required by the incident. • Direct outreach and coordination with targeted/affected entities, and with those who may be targeted or affected. • Activation of Cyber UCG Senior Officials. • Potential need to exercise mutual aid agreements among and between Federal Agencies and non-Federal entities. • Coordinate efforts with all critical departments, agencies, states and organizations, synchronize efforts in accordance with the incident action plan.	• Continue to conduct suggested community activities outlined for Elevated. • Participate, as needed in Cyber UCG activities, including the development of the incident action plan. • Increased levels of event-specific monitoring and communications with the NCCIC and among other participating organizations. • Regular special, event-specific communication or reporting is required, and special information sharing activities. • Evaluate and execute mitigation strategies, as disseminated within the Sector and from DHS, as applicable to reduce organizational risk.

Label	Description	Expected NCCIC Actions	Suggested Community Actions
Critical	Current cyber threat actor behavior, system/hardware vulnerabilities and activities have resulted in the total or near total compromise and disruption across multiple CIKR sectors • Mission-critical cyber systems have been seriously and widely degraded, or destroyed threatening the homeland security, national security or continued operation of government or CIKR functions • Attack methods have no known mitigation methods, or existing response actions are overwhelmed	• NCCIC and the Cyber UCG increase its operational tempo to include frequent scheduled coordination calls with partners and reporting on a more frequent basis, as required by the incident. • Leadership, from the White House to Cyber UCG Senior officials are engaged. • Activation of COOP/COG functions may be necessary. • Activation of ESF-2 and/or other ESFs may be appropriate. • Exercise of mutual aid agreements among and between Federal Agencies and non-Federal entities is essential.	• Continue to conduct suggested community activities outlined for Severe. • Undertake aggressive and collective response efforts as outlined in the incident action plan and in accordance with applicable authorities and capabilities • Evaluate and execute mitigation strategies, as disseminated within the Sector and from DHS, as applicable to reduce organizational risk.

The Secretary of Homeland Security establishes the alert level on the recommendation of the Assistant Secretary for the DHS Office of Cybersecurity and Communications (CS&C) and the Cyber UCG.[15] When determining whether to recommend transitioning to a higher NCRAL level, the Assistant Secretary should consider:

- Whether the conditions outlined in Homeland Security Presidential Directive 5 (HSPD-5) and the National Response Framework (NRF) have been triggered. These include, but are not limited to:
- A Federal department or agency acting under its own authority has requested the assistance of the Secretary of DHS.
- The resources of State, local, tribal, and territorial authorities are overwhelmed, and Federal assistance has been requested by the appropriate State, local, tribal, and territorial authorities.
- More than one Federal department or agency has become substantially involved in responding to the incident.
- The Secretary has been directed to assume responsibility for managing the incident by the President.
- The potential costs of implementing designated security readiness actions. [16]

These same conditions and criteria will be used to evaluate a lowering of the alert level. While the cycle of input, analysis, level determination, and dissemination is a continuous process, at minimum the Assistant Secretary will consider whether or not the NCRAL should be set at a lower level every 24 hours, until it reaches Normal.

Communicating the Alert Level

Once established, the alert level is communicated from the NCCIC to public and private sector partners, including UCG Staff, Senior Officials and their organizations, the White House, the NOC, all CIKR sectors via ISACs, SSAs and the NICC, States[17] and the international community as appropriate. It is also communicated to the public through approved external affairs channels and procedures. This communication will be accompanied by appropriate, specific, and actionable information to include:

[15] The Secretary may choose to delegate setting the NCRAL, especially at lower severity levels.

[16] The participation of federal agencies, CIKR owners and operators, and private sector stakeholders are critical for assessing the implications and potential costs of raising or lowering the NCRAL.

[17] Primarily through the MS-ISAC.

- Conditions or triggers that have been observed or anticipated that justify a change in risk alert level;
- The actual or predicted consequences or impacts that are appropriate to a particular risk alert level;
- Recommended actions that the stakeholder communities should be take; and
- Information and reporting requests from the NCCIC to maintain shared situational awareness.

DHS coordinates the public affairs response at any alert level and the NCCIC External Affairs Officer is responsible for working with the Assistant Secretary for CS&C, Cyber UCG, DHS Office of Public Affairs, White House Communications, Public Information Officers, and National Joint Information Center (NJIC) to communicate to public and external stakeholders.

The NCCIC will continue to develop and refine specific NCRAL procedures, distribution and coordination mechanisms, suggested actions, and detailed descriptions of alert level triggers as part of the NCRAL CONOPS.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Booz Allen Hamilton. (2011). Cyber Operations Maturity Framework. Retrieved September 14, 2011, from http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf

Catalog of Federal Domestic Assistance. (2011). Multi-State Information Sharing and Analysis Center MS-ISAC. Retrieved October 7, 2011, from https://www.cfda.gov/index?s=program&mode=form&tab=step1&id=92a59f59af6aec0232cbe9ff8113557c

Center for Strategic and International Studies. (2008). Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Retrieved August 15, 2010, from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Executive Office of the President. Office of Management and Budget. (2011a). Legislative Language Data Breach Notification. Retrieved September 20, 2010, from http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf

Executive Office of the President. Office of Management and Budget. (2011b). Section by Section Data Breach Notification Analysis. Retrieved August 15, 2010, from http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification-section-by-section-analysis.pdf

Federal Bureau of Investigation. (2010). Cyber Investigations. Retrieved August 18, 2010, from http://www.fbi.gov/cyberinvest/cyberhome.htm

Federal Communications Commission. (2010). Cyber Security. Retrieved August 18, 2010, from http://www.fcc.gov/pshs/emergency-information/cybersecurity.html

Help Net Security. (2010). NIST Draft of Smart Grid Cyber Security Strategy. Retrieved August 17, 2010, from http://www.net-security.org/secworld.php?id=8830

IBM Center for the Business of Government. (2010). Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers. Retrieved September 14, 2010, from http://www.dhses.ny.gov/ocs/resources/documents/Cybersecurity-Management-in-the-States-IBM-Kansas-U-report-May-2010.pdf

Idaho National Engineering and Environmental Laboratory. (2004). Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis. Retrieved November 6, 2010, from https://www.hsdl.org/?view&doc=127068&coll=documents

International Community on Information Systems for Crisis Response and Management. (2010). Empirical Investigation of Alert Notifications: A Temporal Analysis Approach. Retrieved November 6, 2010, from https://www.hsdl.org/?view&doc=128216&coll=documents

Kreisher, Otto. (2009). "Seapower: Collaborative Approach." Special Report. *Port Security* 52, no. 5: 48–50.

Lewis, J. A. (2011). Significant Cyber Incidents Since 2006. *Strategic and International Studies*. Retrieved October 14, 2011, from http://csis.org/files/publication/111020_Significant_Cyber_Incidents_Since_2006.pdf

Library of Congress, Congressional Research Service. (2009). Amber Alert Program Technology. Retrieved November 6, 2010, from https://www.hsdl.org/?view&doc=106554&coll=limited

Library of Congress, Congressional Research Service. (2010). Emergency Alert System (EAS) and All-Hazard Warnings. Retrieved November 6, 2010, from https://www.hsdl.org/?view&doc=117994&coll=limited

McMichael, W.H. (2010). "DoD Cyber Command Is Officially Online." *NavyTimes Online*. Retrieved August 12, 2010, from http://www.navytimes.com/news/2010/05/military_cyber_command_052110/

Multi-State Information Sharing and Analysis Center. (2011). Welcome to the MS-ISAC. Retrieved October 8, 2011, from http://msisac.cisecurity.org/

National Security Council. (2008). The Comprehensive National Cybersecurity Initiative. Retrieved August 1, 2010, from http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

North American Electric Reliability Council. (2002a). Threat Alert System and Physical Response Guidelines for the Electricity Sector: Definitions of Physical Threat Alert Levels: A Model for Developing Organization Specific Physical Threat Alert Level Response Plans. Retrieved November 6, 2010, from http://www.esisac.com/publicdocs/tas_physical_V2.pdf

North American Electric Reliability Council. (2002b). Threat Alert System and Cyber Response Guidelines for the Electricity Sector: Definitions of Cyber Threat Alert Levels: A Model for Developing Organization Specific Cyber Threat Alert Level Response Plans. Retrieved November 6, 2010, from https://www.hsdl.org/?view&doc=9970&coll=documents

Ponemon Institute. (2011). Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies. Retrieved November 12, 2011, from http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

United States Coast Guard. (2009). The State of the Coast Guard Address, Admiral Thad W. Allen. Maritime Operational Threat Response. Retrieved October 12, 2011, from http://www.uscg.mil/history/allen/speeches/docs/SOTCG03032009Transcript.pdf

United States Department of Commerce, National Institute of Standards and Technology. (2008). U.S. Computer Security Incident Handling Guide. Special Publication 800-61, Rev. 1. Retrieved July 10, 2011, from http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

United States Department of Commerce, National Institute of Standards and Technology. (2011). NIST Information Security Glossary of Key Information Security Terms. Retrieved November 20, 2011, from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

United States Department of Homeland Security. (2008). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Retrieved February 15, 2012 from http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

United States Department of Homeland Security. (2008). National Response Framework. Retrieved November 20, 2011, from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

United States Department of Homeland Security. (2009a). National Infrastructure Protection Plan. Retrieved September, 14, 2011, from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

United States Department of Homeland Security. (2009b). Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center. Retrieved October 8, 2011, from http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm

United States Department of Homeland Security. (2010a). Quadrennial Homeland Security Review Report. Retrieved November 20, 2011, from http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

United States Department of Homeland Security. (2010b). DHS Highlights Two Cybersecurity Initiatives to Enhance Coordination with State and Local Governments and Private Sector Partners. Retrieved October 7, 2011, from http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm

United States Department of Homeland Security. (2010c). DHS Works with Partners Across the Country and Around the World to Assess the Nation's Cyber Incident Response Capabilities. Retrieved October 4, 2011, from http://www.dhs.gov/ynews/releases/pr_1285629130041.shtm

United States Department of Homeland Security. (2011a). Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise. Retrieved December 5, 2011, from http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

United States Department of Homeland Security. (2011b). Securing Cyberspace: Our Shared Responsibility. Berkeley, CA: UC Berkeley College of Engineering. Retrieved September, 14, 2011, from http://www.dhs.gov/ynews/speeches/sp_1303766068994.shtm

United States Department of Homeland Security. (2011c). About the National Cybersecurity and Communications Integration Center (NCCIC). Retrieved October 8, 2011, from http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm.

United States Department of Homeland Security. (2011d). Secretary Janet Napolitano's Remarks at the Michigan Cyber Security Summit/National Cyber Security Awareness Month Kick-Off Event. Retrieved August 1, 2010, from http://www.dhs.gov/ynews/speeches/20111007-napolitano-cyber-awareness-month.shtm

United States Department of Homeland Security, Office of Cybersecurity and Communications. (2011). National Cyber Incident Response Plan, Interim Version 1.8. DHS Office of Cybersecurity and Communications.

United States Government Accountability Office. (2010a). Cybersecurity Progress Made But Challenges Remain in Defining and Coordinating the Comprehensive National Initiative, GAO-10-338. Retrieved November 10, 2011, from http://www.gao.gov/new.items/d10338.pdf

United States Government Accountability Office. (2010b). Cyberspace Policy Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, But Sustained Leadership Is Needed, GAO-11-24. Retrieved October 12, 2011, from http://www.gao.gov/new.items/d1124.pdf

United States Government Accountability Office. (2011). Information Security Weaknesses Continue Amid New Federal Efforts to Implement Requirements, GAO-12-137. Retrieved October 11, 2011, from http://www.gao.gov/new.items/d12137.pdf

United States Joint Forces Command. (2011). Interorganizational Coordination During Joint Operations. Joint Publication 3-08. Retrieved September, 14, 2011, from http://www.dtic.mil/doctrine/new_pubs/jp3_08.pdf

University of Pittsburgh Medical Center, Center for Biosecurity. (2009). Closer Look at WHO Pandemic Declaration. Retrieved November 6, 2010, from http://www.upmc-cbn.org/report_archive/h1n1/issue_briefs/2009-06-11-A_Closer_Look_at_WHO_Pandemic_Declaration.html

White House. (2005). The National Strategy for Maritime Security. Retrieved October 18, 2011, from http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf

White House. (2009). Cyberspace Policy Review. Retrieved August 1, 2010, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

White House Office of the Press Secretary. (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure. Retrieved October 4, 2011, from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Williams, Matt. (2009). National Cyber-Security Report Is a Call to Action. *Government Executive*. Retrieved November 6, 2010, from http://www.govtech.com/security/National-Cyber-Security-Report-Is-a-Call.html

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California